Les réseaux sociaux, le droit et les volontés qui les animent

Poullet, Yves; Moiny, Jean-Philippe

Published in:
Social média

Publication date:
2012

Document Version
le PDF de l'éditeur

LES RÉSEAUX SOCIAUX, LE DROIT ET LES VOLONTÉS QUI LES ANIMENT

Jean Philippe MOINY[1] & Yves POULLET[2]

PLAN

1. – INTRODUCTION. DES RÉSEAUX SOCIAUX AUX DROITS DES RÉSEAUX SOCIAUX

Le présent propos introduit la journée. Le rôle assigné à la présentation est présomptueux : il s'agit de mettre en perspective tous les thèmes qui seront traités cette journée ; dans le même temps, il est ingrat car seule l'esquisse est possible dans un tel cadre, là où l'auteur aurait souhaité pouvoir plutôt que soulever des questions, les approfondir voire tenter quelques réponses. Que le participant et le lecteur ne nous tiennent pas rigueur de les laisser ainsi sans conclusions, sachant que les autres contributions y veilleront sans aucun doute. Notre contribution traite des réseaux sociaux (1.1.) et des droits qui s'y appliquent (1.2.).

1.1. – *Les réseaux sociaux*

1. Les « réseaux sociaux » pénètrent de plus en plus et rythment nos vies quotidiennes et nous savons combien nous passons notre temps connectés à leurs services. Les entreprises elles même l'ont compris. Ces réseaux sont devenus un élément essentiel de leur stratégie marketing mais également un outil de communication interne avec et entre les employés. A ce titre, ils sont aujourd'hui l'objet de notre propos. Sans pouvoir disserter ici sur ce que constitue un réseau

(1) Aspirant du F.R.S.-FNRS au CRIDS (FUNDP).
(2) Recteur des FUNDP et Professeur à l'U.Lg.

social, relevons que le concept peut être largement entendu : « *[it] can be defined as [a] website whose main purpose is to act as a connector among users* »[3]. L'European Network and Information Security Agency [ENISA][4] définit le réseau social à partir de ses fonctionnalités de manière un peu plus précise en distinguant ce qui constitue ses composants habituels : « (1) des outils pour afficher de l'information personnelle dans un profil lié à une personne qui comprend ses intérêts et des renseignements sur sa vie privée, (2) des mécanismes pour permettre les interactions personnalisées et sociales, basées autour d'un profil (recommandations, blogues, organisations d'événements sociaux), et (3) des outils pour définir des relations sociales, afin de déterminer qui a accès aux informations disponibles dans les réseaux sociaux et qui sont communiquées avec qui et comment ».

2. Des noms de réseaux sociaux nous viennent spontanément en tête, Twitter, Facebook, Linkedin, Flickr, YouTube, etc. Le réseau social peut être rattaché à une catégorie plus générique de services professionnels ou non offerts par le « cloud computing »[5] ou « informatique en nuages ». Selon le National Institute of Standards and Technology [NIST][6], « le cloud computing est l'accès via le réseau, à la demande et en libre-service, à des ressources informatiques virtualisées et mutualisées. On distingue parmi les services offerts par la technologie du cloud différents services généralement présentés suivant trois niveaux correspondant à des modèles de services »[7] :

- *Software as a Service* (SaaS) : une application informatique est offerte en tant que service ;
- *Platform as a Service* (PaaS) : une plate-forme et des outils de développement sont offerts en tant que service ;
- *Infrastructure as a Service* (IaaS) : les ressources informatiques de bases (processeurs et espace de stockage) sont offerts en tant que service.

(3) A. LEVIN et P. SÁNCHEZ ABRIL, « Two Notions of Privacy Online », *Vanderbilt J. of Ent. And Tech. Law*, 2009, p. 1017.
(4) ENISA, G. HOGBEN (éd.), « Security Issues and Recommendations for online Social Networking », *ENISA Position Paper* n° 1, Octobre 2007, disponible sur www.enisa.europa.eu/activities/identity-and-trust/library/pp/soc-net, p. 6.
(5) Pour un aperçu détaillé de ce que constitue le « *cloud computing* », voy. J.-P. MOINY, « Cloud computing : validité du recours à l'arbitrage ? Droits de l'homme et clauses abusives (partie I) », *RLDI* 2011, 77, pp. 96-99.
(6) Voy. http://www. nist.gov. Sur cette définition, lire Y. POULLET, J.-M. VAN GYSEGHEM, J.-P. MOINY, J. GÉRARD et C. GAYREL, « Data protection in the clouds » in *Computers, privacy and data protection : An Element of Choice*, Springer Verlag, 2010, pp. 377-409.
(7) NIST, P. MELL et T. GRANCE, « The Nist Definition of Cloud computing », septembre 2011, disponible sur http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf, pp. 2-3.

A cet égard, on peut considérer que le réseau Facebook constitue à la fois une offre de SaaS, comprenant une composante d'IaaS, ainsi qu'une PaaS permettant aux développeurs de greffer des applications sur le réseau social. L'ensemble est mis à disposition via Internet à n'importe quel endroit du globe et désormais y compris à partir de nos *smartphones*.

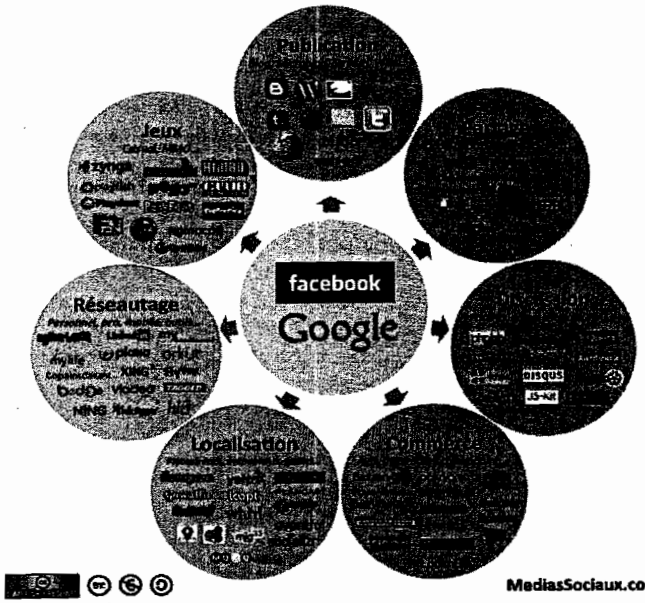
3. Cette réalité des médias sociaux ne peut se comprendre que si on contemple la diversité des applications liées à chaque réseau social[8]. YouTube nous permet de diffuser des videos ou bandes sonores ainsi que d'échanger des commentaires à leurs propos. Second Life est un site de jeux participatifs. Les sites Wiki permettent la diffusion et le partage d'informations susceptibles d'être enrichies par les autres participants. Flickr autorise le partage de photos. Facebook, LinkedIn, MySpace ou Twitter s'ils constituent chacun des sites de communication et de partage à partir d'un profil, ont leurs spécificités propres. Les uns plus à finalité professionnelle, les autres plus grand public, l'un à vocation d'envois de messages courts (micro blogues de type Twitter), les autres n'ayant pas les mêmes contraintes. Par exemple à l'origine en tout cas, Facebook ne s'adressait qu'aux étudiants d'Harvard, université où le plus célèbre des médias sociaux est né. Aujourd'hui, il s'adresse à tous, à tous groupes, et pour tant de finalités et fonctionnalités que nous pouvons parler d'un « meta-réseau social »[9].

Un article récent de Mr. Cavazza[10] permet d'illustrer la diversité des réseaux sociaux à partir de la finalité générale des services rendus (voy. la figure p. 4).

On note la richesse de la palette des services proposés et surtout le fait que des sociétés comme Google et Facebook ont clairement une stratégie « multi-applications », ce qui leur permet de croiser des informations à propos de leurs utilisateurs en provenance de l'utilisation d'applications distinctes, d'enrichir leur connaissance de ceux-ci et d'ainsi accroître la qualité des profils produits par eux et susceptibles d'intéresser des entreprises. Sans aucun doute, une classification proposée par Dominique Cardon permet d'identifier le ou les réseaux

(8) Pour une liste des différents sociaux et une typologiede ceux-ci, lire http://social-buster.blogspot.fr/2012/05/panorama-des-reseaux-sociaux-2012.html.
(9) J.-P. MOINY, « Contracter dans les réseaux sociaux : un geste inadéquat pour contracter sa vie privée, Quelques réflexions en droits belge et américain », *Rev.dr.ULg* 2010, n° 2, p. 135.
(10) F. CAVAZZA, « Panorama des médias sociaux 2011 », 13 décembre 2010, disponible sur http://www.mediassociaux.fr/2010/12/13/panorama-des-medias-sociaux-2011/.

Panorama des médias sociaux 2011

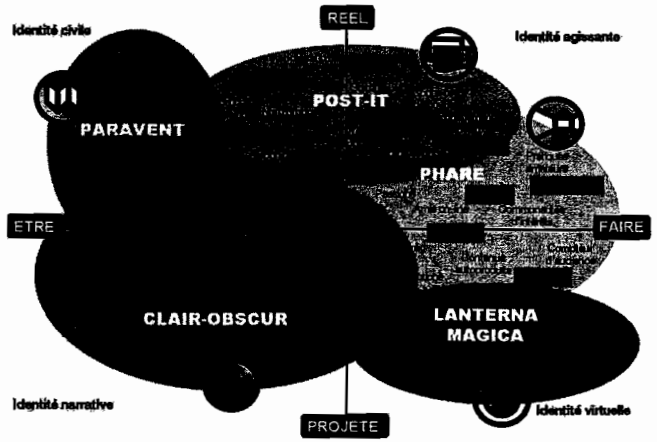


où sont susceptibles d'être décelées les « plus véritables » informations – certainement donc, les plus chères – à propos de leurs utilisateurs. L'auteur, de manière édifiante, classe les réseaux sociaux selon les traits identitaires qu'y projettent les utilisateurs[11] (voy. la figure p. 5).

4. En outre, aux opérateurs des réseaux sociaux s'ajoutent d'autres acteurs : certains proposent aux opérateurs des applications supplémentaires ou complémentaires qui améliorent les services rendus par les opérateurs en tant que cocontractants ou non de ces derniers ; d'autres entendent utiliser les services offerts par l'opérateur ou ces développeurs d'applications pour leurs propres services commerciaux ou non. Par exemple, des entreprises utilisent Facebook comme réseau de communication et de diffusion des messages de l'entreprise et de ses membres, et nombre d'entreprises profitent des réseaux sociaux pour insérer des messages publicitaires ou simplement offrir leurs services. A cet égard, l'article de Cavazza[12], après avoir décrit les différents types de réseaux sociaux, propose la façon dont une entreprise peut utiliser les réseaux sociaux à des fins publicitaires (voy. la figure p. 6).

(11) L'image provient de D. CARDON, « Le design de la visibilité : un essai de typologie du web 2.0 », 2008, disponible sur www.internetactu.net/2008/02/01/le-design-de-la-visibilite-un-essai-de-typologie-du-web-20/. Quant à la contribution complète de l'auteur, voy. D. CARDON, « Le design de la visibilité, Un essai de cartographie du web 2.0 », *La Découverte, Réseaux*, 2008/6, n° 152, pp. 93-137.

Classification des réseaux

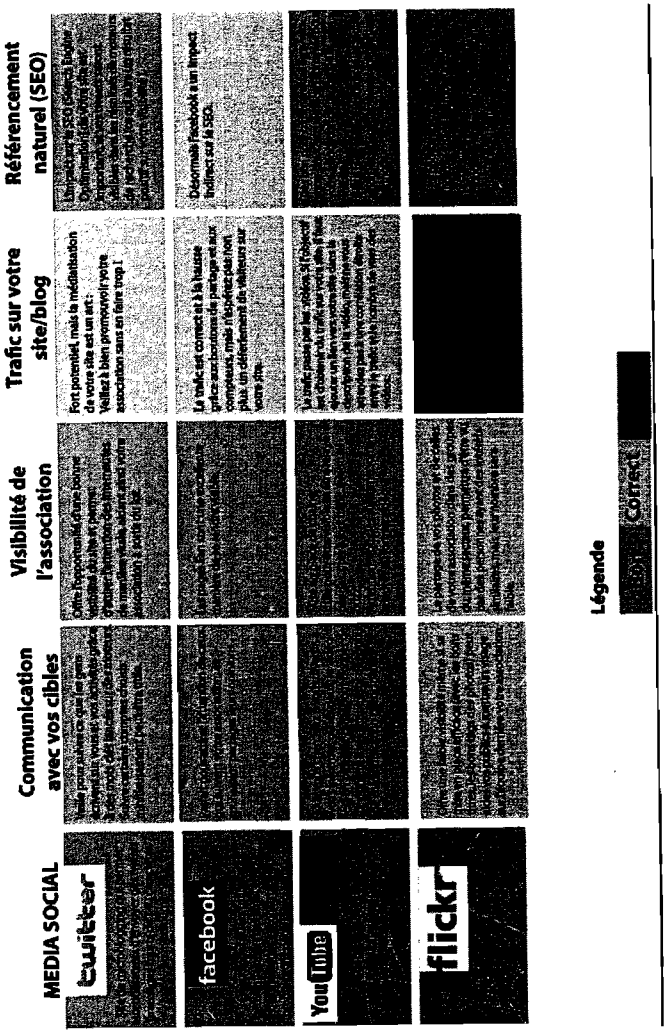


1.2. – *Quels droits pour les réseaux sociaux ?*

5. Notre propos part donc de cette réalité multiple et le titre s'interroge sur la coexistence en droit des différentes volontés qui animent les réseaux sociaux. Comment le droit ou plutôt les droits accordent-ils les intérêts des utilisateurs et fournisseurs des réseaux sociaux ? Si nous utilisons le mot droit au pluriel, c'est tant les questions posées par l'utilisation des médias sociaux se rattachent à de multiples branches du droit. Sur chacune de ces branches, nous nous contenterons de quelques considérations. Nous ajouterons que chaque type de réseau social en fonction des caractéristiques propres de ses applica-

(12) F. CAVAZZA, « Panorama des médias sociaux 2011 », *o.c.*

Guide des médias sociaux



tions et des services offerts, des comportements et des caractéristiques des usagers visés, de la surveillance et du contrôle que l'opérateur du ou des services opère, renvoie à des questions juridiques dont la nature ou la solution peut varier. Par ailleurs, chaque réseau soit dispose de sa propre (auto) régulation, soit renvoie à des textes d'autoréglementation d'associations plus ou moins larges et connues. Cette pratique pose la question de l'intérêt mais également de la valeur de tels textes au regard du droit.

Différentes matières ou branches juridiques ont vocation à régir les divers usages des réseaux sociaux.

- Le droit privé, en priorité le droit des contrats, constitue le socle juridique de base sur lequel est construit le réseau social.
- Nous insistons sur le rôle important des droits de l'homme (vie privée, protection des données – directive 95/46[13], transposée dans la loi vie privée[14] [LVP] et en cours de révision[15], et directive 2002/58[16], la loi sur les communications électroniques en droit belge [LCE][17] –, liberté d'expression, etc.) qui à la fois fondent la libre utilisation des réseaux sociaux, mais dans le même temps, limitent de manière importante l'exploitation de cette utilisation tant par les opérateurs et fournisseurs de services sur ces réseaux que par les autres utilisateurs.
- Le droit du travail trouve également à s'appliquer dans ce contexte : les travailleurs souhaitent utiliser sur les lieux du travail cette ressource communicationnelle y compris pour évoquer leur vie à l'entreprise, mais également se voient invités par leur entreprise à utiliser ces réseaux pour des raisons professionnelles. La fameuse Convention collective de travail n° 81 du 26 avril 2002 relative à la protection de la vie privée des travailleurs à l'égard du contrôle des données de communi-

(13) Dir. (CE) n°95/46 du Parlement et du Conseil du 24 octobre 1995, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données (« directive 95/46 »), *JO* L. 281 du 23 novembre 1995.
(14) Loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel, *MB* 18 mars 1993.
(15) Voy. la Proposition de Règlement du Parlement européen et du Conseil relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données (Règlement général sur la protection des données), COM(2012) 11 final. Pour un commentaire de ce projet, lire L. COSTA et Y. POULLET, « Privacy and the regulation of 2012 », *Computer law and security review*, vol. 28, n° 3, pp. 254-262.
(16) Dir. (CE) n° 2002/58 du Parlement européen et du Conseil du 12 juillet 2002, concernant le traitement de données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques, *JO* L. 201 du 31 juillet 2002.
(17) Loi du 13 juin 2005 relative aux communications électroniques, *MB* 20 juin, 2005.

cation électroniques en réseau s'en trouve particulièrement sollicitée.

- Le droit de la propriété intellectuelle pose à la fois la question de la protection des intérêts des fournisseurs, opérateurs et des entreprises, en particulier par le droit des marques, mais également celle de la protection des utilisateurs qui souhaitent voir protéger les contenus mis sur la toile. On ne manquera pas d'évoquer le rôle de la loi relative au droit d'auteur et aux droits voisins [LDA][18] dans un tel contexte.
- Le droit de la concurrence, qui sans doute pourrait être appelé à jouer un rôle important au regard des situations quasi monopolistiques occupées par certains opérateurs de réseaux sociaux, doit encore être pris en compte. Il importe évidemment d'également évoquer le droit des pratiques du marché et celui de la protection des consommateurs – notamment consacré dans la loi sur les pratiques du marché[19] [LPMPC].
- Le droit pénal, par la prohibition de l'accès non autorisé aux systèmes d'informations (art. 550*bis* du Code pénal), par la répression des atteintes à la considération des personnes (chapitre V, Titre 8 du livre 2 du Code pénal), etc., joue également un rôle sans oublier les questions de plus en plus nombreuses de droit de procédure pénale qui entourent nombre de procès où les autorités policières et judiciaires se trouvent confrontées à des éléments de preuve issus des médias sociaux (*e.g.*, article 46*bis* du Code d'instruction criminelle).
- *Last but not least,* le droit international privé, dans le contexte de réseaux sans frontières à la fois par la qualité des utilisateurs les rejoignant mais également par leur fonctionnement, doit être sollicité dans nombre de litiges afin d'identifier le juge et le droit compétents pour trancher le litige. Nous pensons ici en particulier à certains instruments européens, les Règlements « Rome I »[20], « Rome II »[21] et « Bruxelles I »[22], et

(18) Loi du 30 juin 1994 relative au droit d'auteur et aux droits voisins, *MB* 27 juillet 1994.
(19) L'ancienne loi du 14 juillet 1991 sur les pratiques du commerce et sur l'information et la protection du consommateur, *MB* 29 août 1991, est aujourd'hui remplacée par la loi du 6 avril 2010 relative aux pratiques du marché et à la protection du consommateur, *MB* 12 avril 2010,
(20) Règlement (CE) n° 593/2008 du Parlement européen et du Conseil du 17 juin 2008 sur la loi applicable aux obligations contractuelles, *JO* L. 177, du 4 juillet 2008, ci-après « Règlement Rome I ».
(21) Règlement (CE) n° 864/2007 du Parlement européen et du Conseil du 11 juillet 2007, sur la loi applicable aux obligations non contractuelles, *JO* L. 199 du 31 juillet 2007, ci-après « Règlement Rome II ».
(22) Règlement (CE) n° 44/2001 du Conseil du 22 décembre 2000, concernant la compétence judiciaire, la reconnaissance et l'exécution des décisions en matière civile et commerciale, *JO* L. 12 du 16 janvier 2001, ci-après Règlement « Bruxelles I ».

au Code de droit international privé belge [CDIP][23]. A l'interdisciplinarité juridique, il importe d'ajouter un degré additionnel de complexité : celui de la globalité. Le « *cloud computing* » et les réseaux sociaux reposent généralement sur Internet et mettent à la fois en cause tous les Etats, tous les individus et toutes les entreprises, les uns et les autres ayant des volontés accordées ou désaccordées. Il convient donc souvent et à titre préalable d'identifier les règles applicables. A cet égard, nous pouvons nous demander quelle est l'effectivité d'un droit toujours marqué par un ancrage territorial dans l'attente d'un droit universel ?

Toutes ces règles de droit interagissent, en se limitant, se complémentant ou coopérant, tout en se fondant, le cas échéant, sur des concepts transversaux tels que celui de « consentement ». Elles imposent par ailleurs au juriste un exercice d'interprétation parfois périlleux tant le contexte étudié est évolutif et éprouve les concepts de base de toutes ces disciplines.

6. Le décor est planté. Il nous reste à rentrer dans les quelques considérations juridiques introductives promises. Nous les proposons en deux temps systématiquement fondés sur la volonté des acteurs des réseaux sociaux : le premier temps est celui de la volonté de rejoindre et de quitter le réseau social, une communauté qui se voudrait autorégulée (Titre I). Il s'agit là de deux moments clés qui initient, conditionnent et limitent l'utilisation du réseau social sur laquelle est focalisé le deuxième temps de la réflexion (Titre II). Dans ce premier temps, nous nous interrogeons d'abord sur la liberté de rejoindre et de quitter le réseau social (Titre I, I). Il s'agit ensuite d'étudier la portée que reconnaît le droit au consentement exprimé à l'occasion de l'inscription au réseau social dans le contexte du droit de la vie privée que nous entendrions dans un « sens large » : vie privée, droit à l'image, protection des données, confidentialité des communications électroniques et des systèmes d'information (Titre I, II). Le second temps se focalise sur les différents acteurs du réseau social et leurs ambitions d'utilisation et de contrôle du réseau. Sont envisagés les points de vue de l'utilisateur « de base » (Titre II, I), de l'entreprise (Titre II, II), des autorités publiques (Titre II, III) et

(23) Loi du 16 juillet 2004 portant le Code de droit international privé, *MB* July 27, 2004.

enfin, du fournisseur du réseau social (Titre II, IV). L'ensemble de la discussion permettra d'évoquer ça et là une certaine insécurité juridique des réseaux sociaux et plus largement, du droit des technologies de l'information et de la communication.

2. – ENTRÉE ET SORTIE DU RÉSEAU SOCIAL

2.1. – *La liberté de rejoindre et de quitter une communauté autorégulée*

7. Le droit, en particulier celui des droits de l'homme, envisage de manière positive les réseaux sociaux et leur utilité et prétend donc en faciliter l'accès, sur base de l'article 10 CEDH qui prône la liberté d'expression et de communication. Ainsi la recommandation adoptée le 4 avril 2012 par le Comité des Ministres du Conseil de l'Europe[24] écrit dans son préambule : « [l]es services de réseaux sociaux jouent un rôle considérable dans la vie quotidienne d'un nombre croissant de gens. Ils sont un outil d'expression et de communication directe de masse ou de communication de masse de groupe. Cette complexité offre aux opérateurs de réseaux sociaux ou de plateformes de grandes possibilités de promouvoir l'exercice et la jouissance des droits de l'Homme et des libertés fondamentales, notamment la liberté d'exprimer, de créer et d'échanger des contenus et des idées, et la liberté de réunion. [...] L'importance croissante du rôle des services de réseaux sociaux et des autres services de médias sociaux offre aussi de grandes opportunités pour renforcer la possibilité pour les individus de participer à la vie politique, sociale et culturelle. [...] Ces réseaux sociaux, qui font partie intégrante de la valeur de service public d'Internet, peuvent contribuer à la démocratie et à la cohésion sociale ». Cette qualité de **service public**[25], qui pourrait au-delà de l'Internet être reconnue aux réseaux sociaux, pourrait exiger comme premier devoir des opérateurs de réseaux qu'ils offrent une possibilité pour chacun d'accéder sans discrimination aucune à leurs services et plateformes, en particulier aux personnes handicapées.

Nombre d'internautes entendent, que ce soit pour des raisons professionnelles ou privées, rejoindre les réseaux sociaux et, nous l'avons

(24) Recommandation CM/rec(2012)4 du Comité des ministres aux Etats membres sur la protection des droits de l'homme dans le cadre des services des réseaux sociaux, 4 avril 2012, disponible sur https://wcd.coe.int/ViewDoc.jsp?id=1929465&Site=CM&BackColorInternet=C3C3C3&BackColorIntranet=EDB021&BackColorLogged=F5D383.

dit, l'entreprise n'y échappe pas. A cette fin, il importe de créer un compte[26] et la création de ce compte emporte le consentement à des conditions d'utilisation et politiques de confidentialité préétablies par le fournisseur du réseau social. Ce premier contact avec le réseau social est en principe le moment de la formation d'un **contrat** entre le fournisseur du réseau social et lui-même mais le cas échéant, ce même contrat peut être le lieu de la création de droits et obligations vis-à-vis des autres utilisateurs via le mécanisme de la **stipulation pour autrui**[27]. Ce contrat est souvent un « *clickwrap agreement* », mais il peut également s'agir d'un « *browsewrap agreement* » car le prestataire de service entend que la simple consultation de son site Web vaille acceptation des conditions et politiques précitées[28]. Cette première expression de volonté implique un **consentement** qui est supposé parfaire un contrat ; **l'acceptation** des termes rédigés par le réseau social est supposée les transformer en loi des parties. En vérité, il s'agit d'une **adhésion** pure et simple – le service étant à prendre ou à laisser. Il n'empêche : la figure du contrat d'adhésion est tolérée par le droit depuis bien longtemps maintenant.

8. A ce stade d'adhésion au réseau social, certaines règles protectrices peuvent protéger des utilisateurs particuliers tels que le consomma-

(25) Sur la valeur de service public d'internet, lire la Recommandation CM/Rec(2007)16 du Comité des Ministres aux Etats membres sur des mesures visant à promouvoir la valeur de service public de l'Internet, adoptée le 7 novembre 2007 : « [e]n coopération avec le secteur privé et la société civile, les Etats membres devraient élaborer des stratégies visant à encourager une croissance économique durable, reposant sur des structures de marché compétitives, afin de stimuler les investissements, en particulier de capitaux locaux, dans les ressources essentielles à Internet et aux TIC, notamment dans les zones où les infrastructures d'information et de communication sont peu présentes, plus particulièrement en référence : – à l'élaboration de stratégies qui promeuvent un accès financièrement abordable aux infrastructures de TIC, y compris l'Internet ; – à la promotion de l'interopérabilité technique, de normes ouvertes et de la diversité culturelle dans les politiques de TIC en matière de télécommunications, de radiodiffusion et de l'Internet ; – à la promotion d'une diversité de modèles de logiciels, y compris de logiciels propriétaires, libres et de sources ouvertes ; – à la promotion d'un accès abordable à l'Internet pour les individus, indépendamment de leur âge, leur sexe, leur origine ethnique ou sociale, y compris pour les personnes ou groupes de personnes suivantes : a. ceux ayant de faibles revenus ; b. ceux vivant dans des zones rurales et enclavées ; et c. ceux ayant des besoins particuliers (personnes handicapées, par exemple), en gardant à l'esprit l'importance d'une conception et d'une application spécifique, d'un coût abordable, du besoin de sensibiliser ces personnes ou groupes de personnes, du caractère approprié, attractif, adaptable et compatible des accès et services Internet ; – à la promotion d'un nombre minimal de points d'accès à Internet et aux TIC dans les locaux des pouvoirs publics et, en fonction des besoins, dans d'autres lieux publics, conformément à la Recommandation n° R (99) 14 du Comite des Ministres aux Etats membres sur le service universel communautaire relatif aux nouveaux services de communication et d'information [...] ».

(26) Il faut tontefois relever que les services d'un réseau social peuvent évidemment être publics en ce sens qu'ils sont accessibles aux internautes sans inscription préalable au réseau social. Le site YouTube offre un excellent exemple.

(27) Voy. succinctement dans le contexte des réseaux sociaux, J.-P. MOINY, « Contracter dans les réseaux sociaux : un geste inadéquat pour contracter sa vie privée, Quelques réflexions en droits belge et américain », *o.c.*, p. 224, note de bas de page n° 568.

(28) A propos de ces concepts, voy. J.-P. MOINY, « Contracter dans les réseaux sociaux : un geste inadéquat pour contracter sa vie privée, Quelques réflexions en droits belge et américain », *o.c.*, pp. 181-184.

teur. Un certain **formalisme protecteur**[29] peut ainsi s'imposer. Certes, ce n'est pas le lieu d'insister ici sur les règles imposées par exemple, par la directive européenne dite *e-commerce*[30] et la directive relative aux **contrats à distance** conclus par les consommateurs[31] pertinentes tant en matière d'information préalable, de publicité, de passation de commande et de preuve. Nous renvoyons sur ce point à d'autres nombreux écrits[32]. Limitons-nous juste à un point pertinent et d'actualité. Le consommateur concluant un contrat à distance doit ainsi « recevoir », du prestataire du réseau social « par écrit » ou sur un « support durable », la confirmation de différentes informations – dont le prix et les caractéristiques essentielles du service[33]. A ce sujet, la Cour de justice a récemment jugé à raison qu'il ne suffisait pas de rendre accessible sur un simple site Web[34], via des hyperliens, lesdites informations : dans cette hypothèse en effet, les informations ne sont ni reçues par ni fournies à l'utilisateur, et le site en question ne peut constituer un support durable[35] dans la mesure où on ne peut être sûr qu'il ne fera pas l'objet d'une modification unilatérale de la part du prestataire de service.

Des traces de ce formalisme protecteur apparaissent aussi en droit d'auteur. L'utilisateur peut être amené à céder des droits de **propriété intellectuelle** au fournisseur du réseau social et, le cas échéant, aux autres utilisateurs[36]. D'un réseau à l'autre, une cession de droit

(29) Récemment à ce sujet, voy. H. JACQUEMIN, *Le formalisme contractuel, Mécanisme de protection de la partie faible* Larcier, Bruxelles, 2010.
(30) Dir. (CE) n° 2000/31 du Parlement européen et du Conseil du 8 juin 2000, relative à certains aspects juridiques des services de la société de l'information, et notamment du commerce électronique, dans le marché intérieur, *JO* L. 178 du 17 juillet 2000.
(31) Voy. la Dir. (CE) n° 97/7 du Parlement européen et du Conseil du 20 mai 1997concernant la protection des consommateurs en matière de contrats à distance, *JO* L. 144 du 4 juin 1997, et la Dir. (UE) n° 2011/83 du Parlement européen et du Conseil du 25 octobre 2011 relative aux droits des consommateurs, modifiant la directive 93/13/CEE du Conseil et la directive 1999/44/CE du Parlement européen et du Conseil et abrogeant la directive 85/577/CEE du Conseil et la directive 97/7/CE du Parlement européen et du Conseil, *JO* L. 304, du 22 novembre 2011.
(32) Parmi de nombreux ouvrages, lire M. DEMOULIN, T. DE COSTER, H. JACQUEMIN, E. MONTERO, M. VANDERCAMMEN et T. VERBIEST, *Les pratiques du commerce électronique*, Cahier du CRID, n° 28 Bruxelles, Bruylant, 2007 ; M. DEMOULIN, *Droit des contrats à distance et commerce électronique*, Bruxelles, Kluwer, 2010.
(33) Voy. l'art. 5 § 1er de la Directive 97/7 précitée, et les articles 2.25 et 46 de la LPMPC. A partir du 13 juin 2014, voy. les art. 2.10 et 8 de la Directive 2011/83 précitée.
(34) Il est souligné dans l'arrêt de la Cour qu'existent des sites sophistiqués permettant de garantir l'inaltération de leur contenu ce dont il n'est toutefois pas question dans l'affaire, voy. points 47-49.
(35) La Cour rappelle que le concept de support durable a pour objectif de garantir les fonctions de l'écrit ; il doit permettre au consommateur de posséder les informations en question pour pouvoir faire valoir ses droits : le support doit permettre « de stocker lesdites informations qui lui ont été adressées personnellement » afin de « garanti[r] l'absence d'altération de leur contenu ainsi que leur accessibilité pendant une durée appropriée, et offr[ir] aux consommateurs la possibilité de les reproduire telles quelles », C.J.U.E. 5 juillet 2012 (*Content Services Ltd. v. Bundesarbeitskammer*), *o.c.*, points 42-43.
(36) Sur la question du rôle, de l'interprétation et des limites du consentement en droit d'auteur, lire, A. CRUQUENAIRE, *L'interprétation en droit d'auteur*, Thèse, Larcier, Bruxelles, 2007.

d'auteur peut être plus ou moins pertinente. On imagine – et c'est la règle du jeu – toute la pertinence de la cession de droits d'auteur du moins les droits patrimoniaux, par exemple, dans le cadre de réseaux tel que Wikipédia[37] ou YouTube[38]. Relevons donc en passant le formalisme protecteur belge de la partie réputée faible qu'est l'auteur : à son égard, « tous les contrats se prouvent par écrit »[39]. Et il est satisfait à l'exigence d'un écrit, dans l'ère numérique, « par une suite de signes intelligibles et accessibles pour être consultés ultérieurement, quels que soient leur support et leurs modalités de transmission »[40]. Nous rapprocherons cette exigence de ce qui vient d'être évoqué quant au « support durable », et renverrons ici à d'autres auteurs à propos de la théorie de l'équivalence fonctionnelle[41].

9. Quant au fond du contrat, il va de soi que les conditions d'utilisation des sites de socialisation sont susceptibles de contenir des clauses défavorables à ceux-ci, et il existe des dispositions légales ayant une influence sur le **contenu de la convention**. Nous pensons évidemment au jeu de la prohibition des **clauses abusives** qui constitue une protection particulièrement efficace dont l'entreprise ne peut par définition pas bénéficier[42]. Le **droit d'auteur** peut à nouveau être évoqué. Rappelons que ce que le droit d'auteur entend protéger, ce sont des créations originales de l'esprit humain[43] ; la LDA protège les œuvres qui « revêtent la marque d'une personnalité » ; pour qu'une œuvre soit

(37) Ainsi, un utilisateur de Wikipédia, lorsqu'il publie par exemple un texte dont il est titulaire des droits d'auteur, le place sous deux licences, l'une *creative commons*, l'autre GNU. Voy. http://wikimediafoundation.org/wiki/Conditions_d%27utilisation#7._Licences_applicables_au_contenu, consulté le 22 août 2012.
(38) Le site YouTube comporte ainsi une page spécifiquement dédiée à la question du droit d'auteur, voy. www.youtube.com/t/copyright_center, consulté le 22 août 2012. Concernant la cession des droits, voy. les § 7.2 et 8 des conditions d'utilisation de YouTube, disponibles sur www.youtube.com/t/terms, consulté le 27 août 2012. Sur les différentes licences dites « libres », lire P. LAURENT, « Un logiciel de la Communauté européenne en open source ? Le choix crucial d'une licence libre », *RDTI* 2005, n° 23, pp. 23 et s.
(39) Art. 3, § 1° de la LDA. Sur ce point, lire A. CRUQUENAIRE, *L'interprétation en droit d'auteur*, *o.c.*
(40) Art. 16, § 2, premier tiret de la loi du 11 mars 2003 sur certains aspects juridiques des services de la société de l'information, *MB* 17 mars 2003.
(41) Sur cette notion, la thèse en voie d'achèvement de M. Demoulin, chercheuse au CRID, *Le principe d'équivalence fonctionnelle en droit du commerce électronique*. Pour une définition, celle de V. GAUTRAIS, *Neutralité technologique : rédaction et interprétation des lois face aux technologies de l'information*, Editions Thémis, Montréal, 2012 : « [a]pproche selon laquelle des exigences que l'on retrouve dans certaines lois telles que l'écrit, la signature ou l'original, puissent aussi être appliquées à un support technologique dans la mesure où ces exigences remplissent les mêmes fonctions que l'équivalent papier ».
(42) Voy. les art. 73-78 de la loi du 6 avril 2010 relative aux pratiques du marché et à la protection du consommateur, *MB* 12 avril 2010, et la Dir. (CEE) n° 93/13 du Conseil du 5 avril 1993 concernant les clauses abusives dans les contrats conclus avec les consommateurs, *JO* L. 95, 21 avril 1993.
(43) Voy. F. DE VISSCHER et B. MICHAUX, *Précis du droit d'auteur et des droits voisins*, Bruylant, Bruxelles, 2000, pp. 6-8 et 13-31.

protégeable, « il faut mais il suffit qu'elle soit l'expression de l'effort intellectuel de son auteur, condition indispensable pour [lui] donner [...] le caractère d'individualité nécessaire pour qu'il y ait création »[44]. L'auteur a le droit d'affirmer sa paternité sur une œuvre. Les droits moraux, dont ce droit de paternité, sont parfois rapprochés des droits de la personnalité car « dans l'approche traditionnelle au moins, l'œuvre de l'esprit est avant tout l'émanation d'une personnalité »[45]. Et c'est justement « du lien qui existe entre un auteur et son œuvre » que les droits moraux tiennent leur « force » et leur « singularité »[46] : leur inaliénabilité[47], qui limite ainsi ce que l'utilisateur peut concéder au prestataire du réseau social.

10. Le contrat dont il est question constitue le véhicule juridique d'intégration par le droit des règles auxquelles les parties entendent soumettre le réseau et son utilisation[48] ; telle est la réception de leur **autorégulation**[49]. En réalité, c'est une partie – le fournisseur du réseau social – qui, avec l'aval des autres – les utilisateurs –, le cas échéant conformément aux règles plus ou moins directrices promues par une organisation professionnelle ou un tiers certificateur dont le label, gage de bonnes pratiques, est affiché[50], définit ce qui est ou pas permis. L'espace que l'autorégulation peut occuper ainsi est notamment à la mesure de la place permise par les règles juridiques impératives à la volonté des parties généralement exprimée via leurs consentements à cette autorégulation. C'est en principe le consentement qui, sous l'une ou l'autre appellation selon les règles de droit – consentement, autorisation, accord, etc. – et en fonction des modalités d'expression prescrites plus ou moins strictes, permettra à l'une ou l'autre des parties de réaliser un acte interdit sans qu'il y soit

(44) Cass. 27 avril 1989, *Pas.*, I, p. 909.
(45) A. LUCAS et H.-H. LUCAS, *Traité de la propriété littéraire et artistique*, Litec, 2006, pp. 340-341.
(46) *Ibid.*, p. 343.
(47) Art. 1er, § 2 de la LDA.
(48) Sur le contrat comme mode d'incorporation par le droit de l'autorégulation des entreprises, lire Y. POULLET, *Le droit mode de régulation sociale*, Syllabus, Sources et principes du droit, Namur, Faculté de droit, Tome 1, p. 93.
(49) Sur l'importance de l'autorégulation dans le domaine de la société de l'information, lire la Recommandation n° R(2001)8 sur l'autorégulation des cybercontenus, recommandation du Conseil de l'Europe adoptée par le Comité des ministres le 5 septembre 2001, lors de la 762e réunion des Délégués des Ministres. L'exposé des motifs est particulièrement éloquent à cet égard : « [é]tant donné que l'autorégulation des médias est devenue un mécanisme important et reconnu permettant à ceux-ci d'éviter que les Etats ne légifèrent de manière restrictive en matière de diffusion d'informations par ces médias, en particulier sur les questions de décence et de valeurs morales qui diffèrent largement selon les individus et les Etats, tout en assurant le respect de certaines normes, certains acteurs du secteur des nouveaux services de communication et d'information ont pris l'initiative de créer leurs propres mécanismes d'autorégulation ».
(50) Sur la labellisation des sites, lire D. GOBERT et A. SALAÜN, « La labellisation des sites web : classification, stratégies et recommandations », *DAOR* n° 51, novembre 1999, pp. 83-94.

recouru. Ne pouvant être exhaustifs, nous évoquons au point suivant quelques règles juridiques relatives à la vie privée et particulièrement sollicitées dans le contexte des réseaux sociaux.

11. Enfin avant d'entrer dans ces considérations, arrêtons-nous un instant sur la volonté opposée à celle de rejoindre le réseau : celle de le quitter et de défaire ce contrat qui scellait l'accord des protagonistes. Lorsque l'utilité du réseau social a fait son temps, ou lorsque l'appel d'un autre réseau est irrésistible, l'utilisateur peut souhaiter quitter la communauté en question. Les clauses des conditions d'utilisation permettent généralement cette possibilité ; le prestataire de service et l'utilisateur peuvent unilatéralement rompre la convention. Mais souvent, l'utilisateur est captif : une fois qu'il a tissé son réseau de clients ou de contacts, il est difficilement en mesure de quitter le service sans une perte considérable. En outre, et ce problème est lié au précédent, l'utilisateur peut rencontrer des difficultés à récupérer les informations qu'il a chargées sur le réseau social ou encore à obtenir leur suppression des serveurs du fournisseur du réseau. Ici, lorsqu'il est question de données à caractère personnel, les règles de protection des données sont doublement utiles. D'une part, une fois le réseau quitté, il n'y a en principe plus de raison que son fournisseur conserve les informations liées à l'utilisateur en question. Comme les données ne peuvent être conservées que pour une durée nécessaire à la finalité du traitement réalisé[51] – ici lié à la fourniture d'un service –, dès lors qu'il est mis un terme à l'utilisation du réseau social, il n'y a en principe plus de motif de les conserver. Si nécessaire, l'utilisateur pourra obtenir en justice la **suppression de ces données**[52]. La proposition de règlement européen en matière de protection des données va

(51) Art. 4, § 1er, 5° de la LVP.
(52) Tel que proposé par l'art. 17 du projet de règlement, projet déjà cité : « 1. La personne concernée a le droit d'obtenir du responsable du traitement l'effacement de données à caractère personnel la concernant et la cessation de la diffusion de ces données, en particulier en ce qui concerne des données à caractère personnel que la personne concernée avait rendues disponibles lorsqu'elle était enfant, ou pour l'un des motifs suivants : a) les données ne sont plus nécessaires au regard des finalités pour lesquelles elles ont été collectées ou traitées, b) la personne concernée retire le consentement sur lequel est fondé le traitement, conformément à l'article 6, paragraphe 1, point a), ou lorsque le délai de conservation autorisé a expiré et qu'il n'existe pas d'autre motif légal au traitement des données ; c) la personne concernée s'oppose au traitement des données à caractère personnel en vertu de l'article 19 ; d) le traitement des données n'est pas conforme au présent règlement pour d'autres motifs. 2. Lorsque le responsable du traitement visé au paragraphe 1 a rendu publiques les données à caractère personnel, il prend toutes les mesures raisonnables, y compris les mesures techniques, en ce qui concerne les données publiées sous sa responsabilité, en vue d'informer les tiers qui traitent lesdites données qu'une personne concernée leur demande d'effacer tous liens vers ces données à caractère personnel, ou toute copie ou reproduction de celles-ci. Lorsque le responsable du traitement a autorisé un tiers à publier des données à caractère personnel, il est réputé responsable de cette publication. ».

même un peu plus loin en consacrant un certain **droit à l'oubli**[53] qui élargit et donne effectivité[54] au droit à la suppression des données déjà consacré par la directive de 1995 et notre LVP[55]. D'autre part, la **portabilité des données** est un élément crucial quant à la liberté de l'utilisateur de quitter un réseau pour, le cas échéant, en rejoindre un autre. Pour que le(s) marché(s) du réseau social – encore faudrait-il délimiter ces marchés[56] – fonctionne bien, la portabilité des données est à tout le moins une condition utile. La proposition de règlement consacre son principe[57]. Sans doute, cette portabilité eût-elle pu être exigée sur base du droit de la concurrence et des pratiques du marché mais encore eût-il fallu démontrer la puissance dominante de celui qui emprisonne son utilisateur et l'abus de celle-ci.

2.2. – *Consentement dans les réseaux sociaux et vie privée « au sens large »*

12. Le consentement donné aux conditions d'utilisation est également susceptible de concéder des atteintes aux droits fondamentaux. Il en est par exemple ainsi lorsque l'utilisateur renonce à certaines garanties consacrées dans l'article 6 CEDH, lorsque qu'il accepte de soumettre tous différends à naître à un arbitrage[58]. Il est possible que le fournisseur du réseau social entende donner compétence à une juridiction arbitrale. Par exemple, tel a été antérieurement le cas dans l'hypothèse de Facebook. Aujourd'hui sur le réseau LinkedIn et selon les litiges, les utilisateurs ont le choix – sauf accord contraire des parties – entre la saisine des tribunaux californiens du comté de Santa-Clara ou la saisine d'une juridiction d'arbitrage[59].

(53) A propos du droit à l'oubli, voy. récemment C. DE TERWANGNE, « Internet Privacy and the Right to be Forgotten/Right to Oblivion », *Revista d'Internet, Dret I Politica*, 2012, n° 13, pp. 109-122.
(54) Voir en particulier le point 2 de l'art. 17 (cité note n° 52) qui vise implicitement les réseaux sociaux ayant assuré la publication et la diffusion de données à caractère personnel.
(55) Voy. les articles 12 de la directive 1995/46 et de la LVP.
(56) Pour une tentative succincte d'analyse du contexte du marché des réseaux sociaux, voy. J.-P. MOINY, « Cloud Based Social Network Sites : Under Whose Control ? » in *Investigating Cyber Law and Cyber Ethics*, A. DUDLEY, J. BRAMAN et G. VINCENTI (éds), IGI Global, 2012, pp. 150-153.
(57) C'est l'art. 18 du projet de règlement qui consacre ce nouveau droit : « 1. Lorsque des données à caractère personnel font l'objet d'un traitement automatisé dans un format structuré et couramment utilisé, la personne concernée a le droit d'obtenir auprès du responsable du traitement une copie des données faisant l'objet du traitement automatisé dans un format électronique structuré qui est couramment utilisé et qui permet la réutilisation de ces données par la personne concernée. 2. Lorsque la personne concernée a fourni les données à caractère personnel et que le traitement est fondé sur le consentement ou sur un contrat, elle a le droit de transmettre ces données à caractère personnel et toutes autres informations qu'elle a fournies et qui sont conservées par un système de traitement antomatisé à un autre système dans un format électronique qui est couramment ntilisé, sans que le responsable du traitement auquel les données à caractère personnel sont retirées n'y fasse obstacle. »
(58) Voy. à ce sujet J.-P. MOINY, « Cloud computing : validité du recours à l'arbitrage ? Droits de l'homme et clauses abusives (partie II) », *RLDI* 2012, 78, pp. 100-102.
(59) Voy. le paragraphe 8 des Conditions d'utilisation de LinkedIn, disponible sur www.linkedin.com/static?key=user_agreement&trk=hbft_userag, consultées le 27 août 2012.

Il ne peut être question ici de discuter de toutes ces atteintes et nous limitons ici à étudier la mesure dans laquelle l'assentiment aux conditions d'utilisation et politiques de confidentialité du réseau social est susceptible d'avoir des conséquences en matière de vie privée « au sens large ». Notre propos se limitera à l'analyse de deux points. Le premier a trait à la question de la superposition des droits à l'image et à la protection des données pour couvrir la donnée à caractère personnel que constitue l'image de la personne physique (A) ; le second analyse la question du consentement dans le cadre des législations protégeant la confidentialité des communications électroniques et des systèmes d'information (B).

2.2.1. – *Du droit à l'image vers (ou versus ?) le droit à la protection des données à caractère personnel*

13. Le droit à notre image tellement présente et sollicitée dans le contexte de certains réseaux sociaux permet, nous l'avions souligné, de passer de la propriété intellectuelle à la protection des données à caractère personnel. En effet, l'édifice jurisprudentiel du **droit à l'image** se fonde originellement sur l'article 10 de la LDA qui vient restreindre les droits de l'auteur ou de tout possesseur d'un portrait[60]. Par ailleurs, l'image est au cœur de la protection garantie à tout individu, au titre de la vie privée, par l'article 8 CEDH. La protection des données à caractère personnel, au-delà de ses liens avec le droit fondamental à la vie privée[61], constitue elle-même un droit fondamental consacré dans la Charte des droits fondamentaux de l'Union européenne[62]. Comme la Cour européenne des droits de l'homme vient de le rappeler : « la Cour a souligné que l'image d'un individu est l'un des *attributs principaux de sa personnalité*, du fait qu'elle exprime son originalité et lui *permet de se différencier* de ses pairs. Le droit de la personne à la protection de son image constitue

(60) « Ni l'auteur, ni le propriétaire d'un portrait, ni tout autre possesseur ou détenteur d'un portrait n'a le droit de le reproduire ou de le communiquer au public sans l'assentiment de la personne représentée ou celui de ses ayants droit pendant vingt ans à partir de son décès ».
(61) Nous pouvons considérer qu'elle procède notamment à l'horizontalisation de l'art. 8 CEDH dans le contexte du traitement de données à caractère personnel. Dans son analyse sous l'angle de l'art. 8 CEDH, la Cour européenne des droits de l'homme cite par ailleurs explicitement la Convention n°108 du Conseil de l'Europe pour la protection des personnes à l'égard du traitement automatisé de données à caractère personnel. Voy. notamment CEDH (Gr. Ch.) 16 février 2000, arrêt *Amann v. Suisse*, req. n° 27798/95, § 65. Sur ces liens et le fait que la protection des données constitue une partie intégrante de la protection de la vie privée et qu'il n'y a pas lieu de les dissocier, lire Y. POULLET, « Pour une troisième génération de réglementation de protection des données » in *Défis du droit à la protection de la vie privée : perspectives du droit européen et nord-américain*, coll. Cahiers du C.R.I.D. (n° 31), Bruxelles, Bruylant, 2008, pp. 25-70.
(62) Art. 8 de la Charte des droits fondamentaux de l'Union européenne.

ainsi l'une des conditions essentielles de son épanouissement personnel. Elle présuppose principalement la *maîtrise* par l'individu de son image, laquelle comprend *notamment* la possibilité pour celui-ci d'en refuser la diffusion (Reklos et Davourlis, précité, § 40) »[63] (italiques ajoutés par nous). Ainsi, l'image constitue bien une donnée à caractère personnel au sens de la directive 95/46 et de la LVP la transposant[64] ; *attribut de la personnalité* d'un individu et lui permettant de se *différencier de ses pairs*, elle ne peut être que relative à une personne physique[65] identifiée ou identifiable. Or ne semble pas contestée aujourd'hui la possibilité de commercialiser son droit à l'image ou en d'autres termes, de monnayer, d'une façon ou d'une autre, la *maîtrise* que l'individu a de son image. La Cour inclut en effet *notamment*, dans cette maîtrise, la possibilité de refuser la diffusion d'une image.

14. Par conséquent, les régimes du droit à la protection des données et du droit à l'image s'appliquent cumulativement à l'image[66]. Ainsi, le fondement majeur du traitement de l'image d'une personne doit reposer, que l'on prenne l'un ou l'autre format, sur le **consentement indubitable** – éclairé, libre et spécifique[67],[68] – de la personne concernée. Ce fondement justifie la possibilité d'utilisation voire de la commercialisation, dans une certaine mesure, de la donnée à caractère personnel. Se pose ici la question des relations entre droit à l'image et protection des données. La question est intéressante à plus d'un titre. Nous venons d'en dégager un premier intérêt, celui de l'influence du droit à l'image sur le droit à la protection des données. Le droit à l'image justifierait une certaine commercialisation de la donnée à caractère personnel, même s'il importe d'envisager cette commercialisation avec la plus grande précaution. A l'inverse,

(63) CEDH 7 février 2012, arrêt *Von Hannover v. Allemagne*, requêtes n° 40660/08 et 60641/08, § 96.
(64) Notion dont l'étendue reste discutée. Elle le fut en particulier à propos de l'adresse IP. Il semblerait qu'aujourd'hui la Cour de justice ait tranché la question en considérant que l'IP est bien une donnée à caractère personnel, voy. C.J.U.E. (3e ch.) 24 novembre 2011 (*Scarlet Extended v. SABAM*), aff. C-70/10, § 51. Sur la notion de donnée à caractère personnel, voy. Groupe de travail « article 29 » sur la protection des données, Avis n° 4/2007 sur le concept de données à caractère personnel, 20 juin 2007, WP 136, qui élargit la notion de données à caractère personnel à tonte donnée dont le traitement permet au responsable du traitement d'agir vis-à-vis de la personne concernée. A ce titre, l'adresse IP est certes une donnée à caractère personnel. A propos de l'adresse IP et du débat relatif à son caractère personnel, voy. J.-P. MOINY, « Are Internet protocol addresses personal data? The fight against online copyright infringement », *Computer Law & Security Review*, 27, 2011, pp. 348-361.
(65) S'il est imaginable qu'une personne morale puisse avoir une image au sens de la loi sur le droit d'auteur, les règles de protection des données (sauf et l'exception est importante en matière *d'e-privacy*) ne s'appliquent toutefois pas au traitement des données relatives à des personnes morales.
(66) Un auteur considère que la LVP, lorsqu'elle est applicable, constitue « le fondement exclusif de toute action » visant à protéger l'image J.-F. PUYRAIMOND, « La protection des données personnelles : nouveau fondement du droit à l'image », *AM* 2008, n° 5, p. 364.

l'application des deux régimes peut amener à des résultats différents. Ainsi, sous le régime du droit à l'image, l'image ne semble pouvoir être « prise » et utilisée (diffusée) qu'avec le consentement (tacite ou exprès) de la personne photographiée – sauf peut-être lorsqu'elle n'est que l'accessoire accidentel de la photographie d'un espace public ou lorsqu'elle est une personne publique[69]. Au contraire, en vertu des règles de protection des données, l'image peut également être traitée sur la base d'une balance entre les intérêts du responsable de traitement et ceux de la personne concernée[70].

15. D'autres liens entre les deux régimes de protection pourraient être pointés. Revenons à cette commercialisation légitimée par le consentement d'une donnée à caractère personnel : l'image. Nous touchons ici un point fondamental et bien connu du contexte des réseaux

(67) Chacun de ces termes est défini par l'avis récent donné par le groupe dit de l'art. 29, voy. Groupe de travail « Article 29 » sur la protection des données, « Avis n° 15/2011 sur la définition du consentement », WP187, 13 juillet 2011, disponible sur http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2011/wp187_fr.pdf, ci après « WP187 ». Selon cet avis, pour que le consentement soit *libre*, « il ne doit pas y avoir de risque de tromperie, d'intimidation ou de conséquences négatives importantes pour la personne concernée si elle ne donne pas son consentement. Le traitement de données dans le cadre professionnel, lorsqu'il existe un rapport de subordination, ainsi que dans le cadre de services publics, comme la santé, peut requérir une évaluation approfondie de la question de savoir si les personnes concernées sont libres de donner leur consentement » (p. 39). L'exigence d'un consentement *spécifique* implique qu'un « consentement général, sans précision des finalités exactes du traitement, ne satisfait pas à cette exigence. Plutôt que d'insérer ces informations dans les conditions générales du contrat, il y a lieu de recourir à des clauses de consentement spécifiques, distinctes des conditions générales » (p. 39). Relevons ici que le Groupe 29 avait déjà souligné l'importance de distinguer les clauses relatives à la protection des données des conditions générales à réaliser, et nous en avions souligner l'importance dans le contexte des réseaux sociaux, voy. J.-P MOINY, « Contracter dans les réseaux sociaux : un geste inadéquat pour contracter sa vie privée, Quelques réflexions en droits belge et américain », o.c., p. 216. Le consentement ne peut enfin être *informé* que s'il est satisfait aux obligations d'information consacrées en matière de protection des données (voy. les art. 10 et 11 de la directive 95/46 et l'art. 9 de la LVP). Le Groupe 29 identifie deux exigences supplémentaires. « Premièrement, les informations doivent être transmises dans un langage adapté permettant à la personne concernée de comprendre à quoi elle consent et quelles sont les finalités du traitement. Cette exigence sera fonction du contexte. L'utilisation d'un jargon juridique ou technique excessivement pointu ne répondrait pas aux exigences de la législation. Deuxièmement, l'information fournie aux utilisateurs doit être claire et suffisamment visible afin qu'elle ne puisse pas leur échapper. L'information doit être directement communiquée aux personnes concernées. Il ne suffit pas qu'elle soit simplement disponible quelque par » (p. 40). Ajoutons aussi qu'explicite, le consentement pent fonder le traitement de données à caractère personnel sensibles, voy. l'art. 8, §2, a), de la directive 95/46. En droit belge, ce consentement doit être *écrit*, voy. les art. 6, § 2, a), et 7, § 2, a), de la LVP.
(68) Les règles de protection des données sont ici plus strictes que le droit des contrats quant aux exigences liées au consentement. Ainsi en droit des contrats, pour que les conditions d'utilisation puissent lier l'internaute, il doit les avoir acceptés certainement (de manière tacite ou expresse), sans nécessairement les avoir lu ou en avoir pris connaissance ; il suffit qu'il ait raisonnablement pu en prendre connaissance. A ce sujet, en droit belge et en droit américain, voy. J.-P. MOINY, « Contracter dans les réseaux sociaux : un geste inadéquat pour contracter sa vie privée, Quelqnes réflexions en droits belge et américain », *o.c.*, pp. 195-212.
(69) De manière générale, pour de nombreuses illustrations jurisprudentielles relatives au droit à l'image, voy. B. DUBUISSON, V. CALLEWAERT, B. DE CONINCK et G. GATHEM, *La responsabilité civile, Chronique de jurisprudence 1996-2007, Volume 1 : Le fait générateur et le lien causal*, Larcier, Bruxelles, 2009, pp. 988-993.
(70) Voy. l'art. 5, al. 1e, f), de la LVP.

sociaux et d'Internet en général : l'offre « gratuite » d'un service en échange d'un traitement à finalité publicitaire de données à caractère personnel.

C'est le propre d'un réseau social comme Facebook et bien d'autres, d'offrir une multitude de services tant aux professionnels qu'aux particuliers. Et c'est d'ailleurs, en principe, de la rencontre de ces acteurs que peut être viable économiquement le réseau(71). Ainsi, il est clair que plus s'accroît le nombre d'utilisateurs finaux, plus le réseau devient attractif tant pour ceux-ci dans la mesure où ils peuvent retrouver dans le réseau nombre de leurs « amis », que pour les utilisateurs intermédiaires, ceux qui « vendent » leurs services via le Net et pour les uns et pour les autres. Nous concevons dès lors que le modèle économique gratuité/publicité soit plus largement répandu que celui du réseau social payant, la gratuité rendant l'accès facile aux réseaux qui se paient alors sur une publicité d'autant plus rentable qu'elle peut rencontrer un public large et ciblé d'internautes. Dans l'exemple de Facebook, pour exploiter au maximum cette publicité, les entreprises vont communiquer des messages en fonction de profils anonymes d'utilisateurs recherchés. Pour ce faire, elles créeront ces profils en tenant compte de toute une série de données obtenues par l'analyse des utilisations du réseau : endroit où se trouve le participant au réseau social, choix des mots clés dans l'interrogation des moteurs de recherche, profil public mis sur le net, détection automatique des contenus échangés par la personne, types d'interlocuteurs fréquentés sur la toile. Les données à caractère personnel sont utilisées aux fins publicitaires, en principe par l'opérateur du réseau social qui n'est pas supposé les communiquer aux entreprises concernées. Eu égard aux services offerts en contrepartie, et dans le respect des règles de protection des données – en particulier du principe de proportionnalité –, il faut bien reconnaître qu'aujourd'hui, l'information personnelle constitue, dans une certaine mesure, une « *commodity* »(72), ou un bien « loué » en échange de

(71) Pour une tentative succincte d'analyse du contexte du marché des réseaux sociaux, voy. J.-P. MOINY, « Cloud Based Social Network Sites : Under Whose Control ? », *o.c.*, pp. 150-153.

(72) L'approche selon laquelle la donnée personnelle est considérée comme un « bien » négociable est défendue par de nombreux auteurs, en particulier nord-américains. A propos de ce débat, voy. notamment A. ROUVROY, *Human Genes and Neoliberal Governance, A Foucauldian Critique*, Routledge, 2008, pp. 184-195 ; C. PRINS, « When personal data, behavior and virtual identities become a commodity : Would a property rights approach matter? », *SCRIPT-ed*, vol. 3, n° 4, disponible sur www.law.ed.ac.uk/ahrc/script-ed/vol3-4/prins.asp, pp. 271-303 JANE B. BARON, « Property as Control : The Case of Information », *Mich. Telecomm. Tech. L. Rev.*, 2012, n° 18, pp. 367-418, disponible sur www.mttlr.org/voleighteen/baron.pdf. ; M.J. RADIN, « Market-Inalienability » in *The Ethics of Reproductive Technology*, K.D. ALPERN (éd.), Oxford University Press, 1992, pp. 174-194.

l'utilisation d'un service. Ce que les défenseurs de la vie privée peuvent parfois voir d'un mauvais œil.

16. Dans ce contexte, le groupe de travail « Article 29 » observe que « la complexité des pratiques de collecte des données, des modèles commerciaux, des relations entre fournisseurs et des applications technologiques dépassent, bien souvent, la capacité ou la volonté d'une personne de décider, par un choix actif, de contrôler l'utilisation et le partage d'informations »(73). Il est donc essentiel de préciser et de respecter les limites du consentement et de s'assurer que seul un consentement « résultant d'un comportement non équivoque » est considéré comme tel(74). Une des difficultés rencontrées dans l'application des règles de protection des données résulte de l'origine américaine de nombreux prestataires de réseaux sociaux. Au moment du lancement de leurs services, ils se limitent au marché américain et ne s'intéressent guère au droit étranger. Et cet intérêt pour le droit étranger ne croît pas toujours proportionnellement avec l'expansion de l'offre géographique du service. En ajoutant à cela que les règles de protection des données, notamment, ne sont pas toujours les plus simples à appliquer aux nouveaux contextes technologiques, et que les autorités tardent parfois à réagir, voire n'agissent pas de concert au sein de l'UE – comme dans l'hypothèse de Google Street View par exemple –, nous assistons à l'existence de fait d'une situation susceptible de violer massivement la loi, situation qui est d'autant plus difficile à contester et modifier qu'elle s'est consolidée par le temps.

17. Le consentement souvent évoqué jusqu'ici est celui exprimé au moment de l'inscription sur le réseau social, mais, à de nombreuses autres reprises, l'utilisateur est appelé à consentir et ce point est particulièrement important en matière de protection des données. Ainsi, l'utilisateur consent implicitement mais certainement lorsqu'il choisit – s'il peut choisir – à qui communiquer le contenu qu'il injecte dans le réseau social. En réalité là, plus que consentir, il traite ses propres données et le responsable de traitement n'apparaît plus que

(73) Groupe de travail « Article 29 » sur la protection des données, « L'avenir de la protection de la vie privée – Contribution conjointe à la consultation de la Commission européenne sur le cadre juridique du droit fondamental à la protection des données à caractère personnel », WP168, 1e décembre 2009, p. 19.

(74) Contrôleur européen de la protection des données, « Avis du contrôleur européen de la protection des données du 14 janvier 2011 sur la communication de la Commission 'Une approche globale de la protection des données à caractère personnel dans l'Union européenne', *JO* C. 180, du 22 juin 2011, point 82.

comme un sous-traitant[75]. Il est susceptible de consentir aux modifications des pratiques du fournisseur du réseau social, et il consent encore, lorsqu'il accepte de greffer à son profil – ou à son *smartphone* – des applications tierces, à ce que les développeurs de celles-ci puissent utiliser certaines données. Ces consentements devront évidemment être jugés valides pour être assortis d'effets juridiques. Pour ne prendre qu'un exemple, lorsque le fournisseur du réseau social entend changer certaines règles du jeu – modification des paramètres de diffusion de l'information ou des traitements de données qu'il entend opérer pour son compte ou le compte de tiers, il ne peut se limiter à prévoir que continuer d'utiliser le site constitue un consentement à ces nouvelles conditions. Lorsque l'utilisateur est déjà inscrit et captif pour diverses raisons[76], les règles de **protection des données** ont un ***effet cliquet*** : il ne peut être ici fait appel au consentement de l'utilisateur que s'il a la possibilité de maintenir le jeu des anciennes règles[77]. Dans le cas contraire, un tel consentement n'est pas libre et la modification « quasi-unilatérale » opérée, s'il elle ne peut être fondée autrement, est illicite. Relevons que dans un *order* récemment adressé à Facebook par la Federal Trade Commission américaine, la Commission exige que Facebook « *obtain the user's affirmative express consent* » « *prior to any sharing of a user's nonpublic user information by [Facebook] with any third party, which materially exceeds the restrictions imposed by a user's privacy setting(s)* »[78].

2.2.2. – *Confidentialité des communications électroniques et des systèmes d'information*

18. Le même consentement que celui évoqué précédemment en matière de protection des données est aussi susceptible de lever la

(75) Lorsque l'utilisateur maîtrise techniquement ce qu'il advient de l'information aur le réseau et qui peut y accéder, il agit de son propre chef en se servant d'une simple application informatique (comme un blog) dont le prestataire peut être vu comme un sous-traitant. Par contre, dès que le prestataire du service traite les données à caractère personnel d'une manière que ne maîtrise – contrôle – pas l'utilisateur (en requérant, le cas échéant, le consentement de ce dernier) – par exemple en communiquant les informations à un tiers ou en enregistrant, pour son compte, ces données –, il peut alors devenir responsable de traitement.

(76) Voy. J.-P. MOINY, « Cloud Based Social Network Sites : Under Whose Control ? », *o.c.*, pp. 163-164.

(77) Ajoutons que la « spécificité du consentement signifie également que si les finalités du traitement de données par le responsable du traitement changent à un moment donné, l'utilisateur doit en être informé et être mis en mesure de consentir à ou aux nouvelles finalités du traitement. Les informations fournies doivent, notamment, expliquer les conséquences entraînées par un refus des changements proposés », WP187 précité.

(78) U.S. F.T.C., *In the matter of* FACEBOOK, Decision and Order, 27 juillet 2012, disponible sur http://ftc.gov/os/caselist/0923184/120810facebookdo.pdf.

confidentialité des communications électroniques[79] qui cette fois, protège également les personnes morales[80]. En droit européen, la confidentialité des communications électroniques relève des règles relatives à la protection des données à caractère personnel dans le secteur des communications électroniques[81]. Dans le contexte des réseaux sociaux et du « *cloud computing* », ces règles sont d'application dès lors que les services en question sont offerts via Internet. La protection des communications électroniques constitue la première étape de protection du contenu communiqué par l'utilisateur – il envoie des données vers un serveur. En transit *et jusqu'à l'arrivée à destination*, les communications sont protégées contre toute intrusion d'un tiers dont le prestataire de services intermédiaires – tels que le fournisseur du réseau social, le fournisseur d'accès à Internet, etc. Le fournisseur du réseau social peut souvent être considéré comme un tiers par rapport au contenu de nombreuses communications électroniques dans la mesure où il n'est pas le destinataire de celles-ci et n'est qu'un intermédiaire technique même si parfois il peut être destinataire de certaines communications. Il en est par exemple ainsi lors de l'inscription sur le réseau social, lorsque l'utilisateur complète les champs obligatoires. Il en est de même lorsque la communication électronique en question est une requête permettant l'utilisation du site Web (*e.g.*, consultation du profil d'un autre utilisateur). Dans ces hypothèses, le contenu, le message, de la communication, est bien adressé au fournisseur du réseau social.

Certes, l'opérateur d'un réseau social *n'est pas* un fournisseur de service de communications électroniques[82] mais il offre en tous cas

(79) Voy. l'art. 314*bis* du C.pén. qui évoque le consentement des participants à la communication, et l'art. 124 de la LCE qui prend quant à lui en compte l'autorisation des personnes (directement ou indirectement) concernées par la communication.

(80) Il s'agissait d'ailleurs là, à l'époque de l'adoption de la directive 2002/58, d'une nouveauté en matière de protection des données, voy. l'art. 1°, § 2, de la directive 2002/58.

(81) Voy. l'art. 5 de la directive 2002/58 depuis modifiée par la directive du 28 octobre 2009 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques (directive dite e-privacy).

(82) En principe, se sont ici les fournisseurs d'accès à Internet du prestataire du réseau social et de l'utilisateur qui sont des fournisseurs de services de communications électroniques. Selon l'art. 2, c), de la Dir. (CE) n° 2002/21 du Parlement européen et du Conseil dn 7 mars 2002 relative à un cadre réglementaire commun pour les réseaux et services de communications électroniques (directive « cadre »), *JO* L. 108, du 24 avril 2002, un service de communications électroniques est « le service fourni normalement contre rémunération qui consiste entièrement ou principalement en la transmission de signaux sur des réseaux de communications électroniques, y compris les services de télécommunications et les services de transmission sur les réseaux utilisés pour la radiodiffusion, mais qui exclut les services consistant à fournir des contenus à l'aide de réseaux et de services de communications électroniques ou à exercer une responsabilité éditoriale sur ces contenus ; il ne comprend pas les services de la société de l'information tels que définis à l'art. 1er de la directive 98/34/CE qui ne consistent pas entièrement ou principalement en la transmission de signaux sur des réseaux de communications électroniques ».

un service de la société de l'information[83] et certaines règles protectrices des communications électroniques lui sont applicables. Nous relèverons aussi que la protection d'une communication électronique non destinée au prestataire de service subsiste lorsqu'elle est stockée sur les serveurs de ce dernier, à condition qu'elle ne soit pas adressée à une audience *indéterminée* et *fluctuante*[84].

19. Les informations une fois stockées dans un système d'information – un terminal quel qu'il soit (serveur du réseau social, ordinateur personnel de l'utilisateur, etc.) –, sont protégées contre tout accès non autorisé – ***hacking***[85]. Si le *hacking* ou l'accès non autorisé est sanctionné pénalement par des dispositions spécifiques, le droit à la vie privée pourrait également et de manière opportune le prévenir, considérant à juste titre que l'intrusion dans un système d'information privé peut être jugée comme la violation d'un « domicile » certes virtuel, protégé par l'article 8 de la CEDH. A ce sujet, l'opinion d'un juge américain – certes dissidente – peut opportunément être citée : « *for most people, their computers are their most private spaces. People commonly talk about the bedroom as a very private space, yet when they have parties, all the guests — including perfect strangers — are invited to toss their coats on the bed. But if one of those guests is caught exploring the host's computer, that will be his last invitation. There are just too many secrets on people's computers, most legal, some embarrassing, and some potentially tragic in their implications [...] Emails and history links may show that someone is ordering medication for a disease being kept secret even from family members. [...] Or a married mother of three may be carrying on a steamy email correspondence with an old high school boyfriend. Or an otherwise respectable, middle-aged gentleman may be looking at dirty pictures* »[86]. D'une importance indiscutable pour son utilisateur, le terminal – dans le contexte des réseaux sociaux, son ordinateur personnel et/ou son téléphone mobile –, nous l'avons déjà

(83) Ce type de service étant défini comme « tout service presté normalement contre rémunération, à distance par voie électronique et à la demande individuelle d'un destinataire de services », art. 1er, 2), *a*), de la directive (CE) n° 98/48 du Parlement européen et du Conseil du 20 juillet 1998, portant modification de la directive 98/34/CE prévoyant une procédure d'information dans le domaine des normes et réglementations techniques, *JO* L. 217, 5 août 1998. En droit belge, voy. l'art. 2, 1° de la Loi du 11 mars 2003 sur certains aspects juridiques des services de la société de l'information, *MB* 17 mars 2003.

(84) Elles le sont d'abord dans une première phase de communication : celle de l'envoi de la communication à l'opérateur du réseau social. Pour une justification détaillée en droit européen et en droit belge de la position proposée ici, voy. J.-P. MOINY, « Cloud Based Social Network Sites : Under Whose Control ? », *o.c.*, pp. 168-172.

(85) Voy. l'art. 550*bis* du C.pén.

(86) U.S. Court of Appeals for the Ninth Circuit, 9 mars 2006 (*United States of America v. Micah J. Gourde*), 440 F.3d 1065, disponible sur www.altlaw.org/v1/cases/1378436, opinion dissidente du juge Kleinfeld.

estimé, peut être considéré comme au cœur d'une troisième génération de réglementation de protection des données[87]. La Cour constitutionnelle allemande a reconnu récemment l'existence d'un nouveau droit fondamental à « la confidentialité et l'intégrité des systèmes d'information technologiques », qu'elle fonde sur le droit général à la personnalité[88].

Le terminal de l'utilisateur et les serveurs du fournisseur de réseau social sont par ailleurs explicitement protégés par l'article 5.3 de la directive e-privacy de 2009 déjà citée contre toute intrusion non autorisée ou plutôt suspendus à l'accord du titulaire du terminal qu'il s'agisse d'une puce RFID, d'un ordinateur ou d'un téléphone mobile[89]. Ainsi par exemple, avec *l'accord*[90] de l'utilisateur, un *cookie* pourra être placé sur son terminal[91].

C'est également avec *l'autorisation* du fournisseur du réseau social que les développeurs d'applications et utilisateurs « de base » peuvent accéder aux serveurs et aux données qu'ils contiennent[92]. En d'autres termes, cette autorisation, qui renvoie à la volonté des parties mais est susceptible d'être autre chose que le consentement en matière de protection des données, est également susceptible d'être requise à l'occasion de l'inscription de l'utilisateur.

3. – UTILISATION ET CONTRÔLE DU RÉSEAU SOCIAL

Une fois que les différents protagonistes se sont accordés quant à l'accès au réseau social, chacun entendra l'utiliser et le contrôler à ses fins propres. Sans être exhaustif, l'individu consommateur (ou pas) – que nous qualifions ci après d'utilisateur « de base » (3.1.) – et l'entreprise « utilisateur » du réseau social (3.2.) à la fois comme destinataire des services offerts par l'opérateur mais également comme offrant grâce à ces services des services supplémentaires aux utilisateurs de base, sont les deux utilisateurs principaux du réseau

(87) Y. POULLET, « Pour une troisième génération de réglementation de protection des données », *o.c.*, pp. 62-65.

(88) P. DE HERT, K. DE VRIES et S. GUTWIRTH, note d'observation sous Cour constitutionnelle fédérale allemande, 27 février 2008, *RDTI* n° 34, 2009, pp. 87-92.

(89) Pour un commentaire de cette disposition, voy. Y. POULLET in *Concise European IT Law*, 2nd éd., A. BÜLLESBACH, S. GIJRATH, Y. POULLET et C. PRINS (éds), Wolters Kluwer, 2010, pp. 196-199.

(90) Voy. l'art. 5, § 3, de la directive 2002/58. En droit belge, il incombe d'obtenir son consentement, voy. l'art. 129 de la LCE.

(91) Le rapport explicatif de la Convention n° 185 du Conseil de l'Europe sur la cybercriminalité (« Convention de Budapest »), spécifie toutefois que « l'utilisation des outils standard prévus dans les protocoles et programmes de communication courants n'est pas en soi 'sans droit', en particulier lorsque le détenteur du droit d'accès au système visé est réputé avoir accepté cette utilisation, comme dans le cas des 'cookies' en s'abstenant de refuser la première livraison ou de l'éliminer », § 48.

(92) Voy. l'art. 550*bis* du C.pén.

social[93]. Les autorités publiques en sont un troisième moins visible (3.3). Et bien entendu, le fournisseur du réseau lui-même ne peut être oublié (3.4).

3.1. – *L'utilisateur « de base »*

20. L'utilisateur « de base » peut placer les contenus que lui permettent les formats choisis par les opérateurs. Ainsi, le contenu peut être limité (Twitter) ou non (Facebook)[94], il peut concerner un public déterminé d'amis ou plus large, voire toute personne qui aurait accès au réseau de l'opérateur. La liberté d'expression fonde souvent l'utilisation sans contrôle a priori des services de partage de contenus ou de diffusion de notre pensée, que la diffusion en soit limitée ou non. Et nous savons combien la Cour européenne des droits de l'homme entend protéger au titre de l'article 10 CEDH ce qui favorise le débat public à propos d'une question d'intérêt général[95]. Le réseau social est un canal privilégié d'exercice de la liberté d'expression des utilisateurs, et il favorise également le débat politique et la liberté d'association[96].

21. Le Conseil de l'Europe en même temps qu'il rappelle et promeut cette liberté dont l'effectivité se trouve accrue sans commune mesure par les technologies de l'information et en particulier les réseaux sociaux[97], souligne les limites de cette liberté : « [s]e référant aux

(93) Cette énumération n'est toutefois pas exhaustive. Il importe également de relever que les politiciens sont également utilisateurs des réseaux sociaux, tout comme diverses associations à finalités politique, sociale, ou autres, mais qui ne peuvent être incluses dans le concept d'entreprise.

(94) Etant entendu que *contractuellement*, le fournisseur du réseau social entendra tout de même limiter du moins en partie les types de contenus diffusés.

(95) Voy. le premier attendu de la Recommandation CM/Rec(2012)4 du Comité des Ministres aux Etats membres sur la protection des droits de l'homme dans le cadre des services de réseaux sociaux adoptée le 4 avril 2012 : « [l]es services de réseaux sociaux jouent un rôle considérable dans la vie quotidienne d'un nombre croissant de gens. Ils sont un outil d'expression et de communication entre individus, mais aussi un outil de communication directe de masse ou de communication de masse de groupe. Cette complexité offre aux opérateurs de services de réseaux sociaux ou de plateformes de grandes possibilités de promouvoir l'exercice et la jouissance des droits de l'homme et des libertés fondamentales, notamment la liberté d'exprimer, de créer et d'échanger des contenus et des idées, et la liberté de réunion. Les services de réseaux sociaux peuvent aider le grand public à recevoir et à communiquer des informations. »

(96) Voy. notamment P. SWIRE, « Social Networks, Privacy, and Freedom of Association : Data Protection vs. Data Empowerment », *North Carolina Law Review* 2012, vol. 90, pp. 101-143.

(97) A ce propos la récente Résolution 1877 (2012) de l'Assemblée parlementaire du Conseil de l'Europe adoptée le 25 avril 2012, « La protection de la liberté d'expression et d'information sur l'internet et les médias en ligne », disponible sur http://assembly.coe.int/ASP/Doc/XrefViewPDF.asp?FileID=18323&Language=FR. Au point 3 de cette résolution, l'Assemblée « se félicite aussi des nouvelles possibilités offertes aux particuliers de partager publiquement, grâce à l'internet et aux médias en ligne, des informations d'intérêt public, par exemple sur les dysfonctionnements du pouvoir, la corruption et la criminalité organisée, ainsi que sur les violations des droits de l'homme. A cet égard, l'Assemblée apprécie les efforts des journalistes et des médias pour recueillir, analyser et diffuser avec profcssionnalisme les informations brutes fournies par des sources provenant de l'internet. »

articles 10, paragraphe 2, et 17 de la Convention, l'Assemblée rappelle cependant qu'aucun Etat, groupe ou personne ne peut exercer la liberté d'expression et d'information au détriment des droits et libertés reconnus par la Convention, notamment le droit à la vie, le droit à un procès équitable, le droit au respect de la vie privée et le droit à la protection de la propriété. L'Assemblée insiste fortement sur l'article 20 du Pacte international relatif aux droits civils et politiques des Nations Unies, qui stipule que toute propagande en faveur de la guerre et que tout appel à la haine nationale, raciale ou religieuse constituant une incitation à la discrimination, à l'hostilité ou à la violence sont interdits par la loi »[98].

22. Parmi ces limites à la liberté d'expression, la protection de la vie privée et des données revêt un intérêt particulier dans le contexte des réseaux sociaux tant ils sont le lieu de l'exposition des individus aux yeux de tous. Ainsi, selon la qualité de son audience, selon le degré de publicité de son profil, l'utilisateur d'un réseau social sera tenu ou non de respecter les règles de **protection des données** lorsqu'il communique des données à caractère personnel ; il peut devenir un responsable de traitement. La Cour de justice, dans l'affaire *Lindqvist*, a déjà jugé que la diffusion de données à caractère personnel à un nombre *indéfini* de personne via Internet ne pouvait relever de l'exclusion au champ d'application des règles de protection des données[99] – la fameuse ***« household exemption »***. Une communication de données à caractère personnel au public des internautes ne peut être une activité exclusivement personnelle. On peut se demander si *a contrario,* lorsqu'un profil est « fermé », autrement dit qu'il est nécessaire d'être autorisé par l'utilisateur pour y accéder, le nombre de personnes accédant aux données étant *défini*, l'utilisateur en question devrait pouvoir être exclu du champ d'application de la protection des données. C'est probablement aller un peu vite que de raisonner ainsi, et c'est surtout méconnaître la réalité. On regrette que la proposition de règlement en matière de protection des données n'apporte pas de solution praticable à cette question brûlante et actuelle[100]. On renverra à une tentative de solution du problème qui avait été récemment proposée –

(98) Résolution 1877 (2012) de l'Assemblée parlementaire du Conseil de l'Europe adoptée le 25 avril 2012, *o.c.*, point 5.

(99) Voy. C.J.C.E. 6 novembre 2003 (*Procédure pénale v. Bodil Lindqvist*), aff. C-101/01.

(100) Voy. l'art. 2, § 2, d), du projet de règlement.

et puis abandonnée (temporairement ?) – au Conseil de l'Europe[101].

23. L'affaire *Lindqvist* nous amène à développer rapidement la question des flux transfrontières dont la réglementation en matière de protection des données est soumise à un régime spécifique. Toute mise à disposition sur un réseau social n'est-il pas du fait de son accessibilité aux quatre coins de la planète un flux transfrontières ? La question est délicate et mériterait à elle seule une contribution d'ampleur. Contentons-nous sur ce point d'évoquer et de critiquer la solution donnée par la Cour de Justice de l'Union européenne dans l'affaire *Lindqvist*. La Cour y a jugé que la communication de données à caractère personnel via un site Internet ne constituait pas un flux transfrontière de données à caractère personnel. Or qu'y a-t-il aujourd'hui de plus transfrontière qu'Internet et le « *cloud computing* » n'échappe pas à la règle de l'internationalité puisqu'il tire son avantage des facilités offertes par l'Internet. Pourtant, la Cour juge dans cette affaire que *Mme Lindqvist* – et la Cour ne se prononce qu'à son égard –, en chargeant des données sur les serveurs de son hébergeur, *situé sur le territoire de son Etat membre de résidence* (*quid* s'il s'était agi d'un hébergeur sis sur un autre Etat membre comme c'est le cas actuellement des réseaux sociaux dont le serveur est quelque part... dans les nuages[102] ?) ne réalise pas un flux transfrontière de données. Faut-il tirer de ce raisonnement que c'est alors l'hébergeur qui réaliserait ce flux dans la mesure où les données communiquées ou confiées à lui le sont pour être rendues accessibles à tout internaute ? Cette conclusion heurte le bon sens. L'hébergeur n'est-il pas dans cette opération de transmission de l'information qu'un simple sous-traitant de l'utilisateur qui poste le message ? Bref les interprétations que l'on peut donner à la décision sont insatisfaisantes d'un point de vue juridique.

Ce que l'on comprend, c'est que la Cour a entendu exclure l'individu qui publie des données sur Internet du régime des flux transfrontières de données, probablement pour des raisons politiques, parce qu'elle considèrerait que le régime des flux transfrontières,

(101) Voy. T-PD-BUR, « Moderniser la Convention : nouvelles propositions », 27 avril 2012, disponible sur www.coe.int/t/dghl/standardsetting/dataprotection/TPD_documents/T-PD-BUR_2012_01Rev2FIN_fr.pdf, art. 3, § 1*bis* : « La présente Convention ne s'applique pas aux traitements de données effectués par une personne physique pour l'exercice d'activités exclusivement personnelles ou domestiques, *à moins que les données ne soient rendues accessibles à des personnes ne relevant pas de la sphère personnelle ou domestique* » (italique ajouté par nous).

(102) A l'origine sur Facebook, les données étaient toutes traitées aux Etats-Unis. En application donc de la jurisprudence *Lindqvist*, un utilisateur de Facebook transmettait bien les informations à un prestataire de service situé sur le territoire d'un Etat tiers, réalisant par là un flux transfrontière de données.

appliqué à un internaute qui poste un message et non à une entreprise dont c'est l'activité, excessif. Si l'objectif de non application du régime est compréhensible, peut-être d'autres solutions eussent pu être trouvées. Ainsi, la directive 95/46 – et dans une certaine mesure, également le projet de règlement actuellement en discussion – prévoient que les Etats membres disposent d'une large marge d'appréciation pour rendre souple et praticable la réglementation de la publication d'informations à caractère personnel sur Internet dans le cadre de l'exercice légitime de la liberté d'expression. On sait que grâce à la jurisprudence de la Cour européenne des droits de l'homme, le journalisme n'a jamais été aussi bien protégé. En outre, ne fallait-il pas à l'heure où l'évolution des technologies contraint à des modifications des règles de protection des données, que le législateur se saisisse de cette question de la définition du flux transfrontière de données ? Lors des discussions relatives à la révision de la Convention n° 108, la question de cette modification a été abordée au Conseil de l'Europe mais n'a pu aboutir[103].

24. Toujours sous l'angle de la protection des données et de la vie privée, en particulier du **droit à l'autodétermination informationnelle**[104], l'individu souhaite maîtriser les limites de la diffusion des données le concernant[105]. La place reconnue par le droit à son

(103) Voy. T-PD-BUR, « Moderniser la Convention : nouvelles propositions », *o.c.*, art. 12, § 1° : « Chaque Partie veille à ce que les données à caractère personnel ne soient *communiquées ou rendues accessibles* à un destinataire ne relevant pas de sa juridiction qu'à la condition qu'un niveau adéquat de protection des données à caractère personnel soit assuré » (italique ajouté par nous).

(104) Sur ce droit consacré dès 1983 par la Cour constitutionnelle allemande, lire Y. POULLET et A. ROUVROY, « Le droit à l'autodétermination informationnelle et la valeur du développement personnel : une réévaluation de l'importance du droit à la protection de la vie privée pour la démocratie in *Etat de droit et virtualité* », Thémis, Montréal, pp. 157-222.

(105) De manière générale, à propos de la protection des données dans les réseaux sociaux, lire la Recommandation CM/Rec(2012)4 du Comité des Ministres aux Etats membres sur la protection des droits de l'homme dans le cadre des services de réseaux sociaux dont on extrait les passages suivants : « 12. Les services de réseaux sociaux traitent un nombre considérable de données à caractère personnel, y compris les données relatives au profil des internautes et à leur utilisation d'internet. Des tiers, comme les employeurs, les compagnies d'assurance, les autorités chargées de l'application de la loi et les services de sécurité, sont notamment susceptibles d'accéder aux données à caractère personnel publiées dans un profil. 13. Les données à caractère personnel ne devraient pas être traitées par les services de réseaux sociaux au-delà de la finalité légitime particulière pour laquelle elles ont été collectées. Ces services devraient limiter le traitement aux seules données strictement nécessaires pour parvenir à la finalité convenue et pour une durée aussi courte que possible. 14. Les services de réseaux sociaux devraient demander le consentement éclairé des utilisateurs lorsqu'ils souhaitent traiter de nouvelles données à leur sujet, partager leurs données avec d'autres catégories de personnes ou d'entreprises et/ou utiliser leurs données à des finalités autres que celles spécifiées lors de leur collecte initiale. Comme le précise la Recommandation CM/Rec(2010)13 sur la protection des personnes à l'égard du traitement automatisé des données à caractère personnel dans le cadre du profilage, les utilisateurs devraient être informés de l'utilisation de leurs données personnelles à des fins de profilage. La décision de l'utilisateur (refus ou consentement) ne devrait avoir aucune incidence sur son accès au service en question. Lorsque des applications tierces permettent l'accès de tiers aux données à caractère personnel des utilisateurs, les services concernés devraient proposer suffisamment de types d'accès de plusieurs niveaux (« multi-layered ») de manière à ce que les utilisateurs puissent spécifiquement consentir à l'accès à différentes catégories de données. »

consentement, évoquée préalablement[106], poursuit notamment cet objectif ; en soumettant le traitement de données à la volonté de l'individu, celui-ci peut maîtriser ce qu'il advient des données le concernant. Le consentement n'est toutefois pas – et heureusement – la seule base de légitimité de traitement des données à caractère personnel[107]. Outre la place offerte à la volonté de l'individu – qui va au-delà de la protection des données –, celui-ci dispose vis-à-vis de tout responsable de traitement – fournisseur du réseau social ou autre utilisateur – du droit de savoir que des données sont traitées à son sujet, du droit d'y **accéder** (et d'en obtenir copie) et du droit de connaître la logique qui sous-tend le traitement de données – à tout le moins lorsque la personne concernée est soumise à des décisions automatisées[108]. Le droit de connaître cette logique se révèle particulièrement pertinent lorsqu'il est question de profilage[109]. Il a été tenté d'en introduire une version étendue dans la Convention 108 du Conseil de l'Europe, tant ce droit est essentiel, et on déplore sa réduction dans le projet de règlement européen[110]. Toujours sous l'angle du droit d'accès la Cour de justice a par ailleurs rappelé avec quelques précisions additionnelles que la personne concernée avait également le droit de connaître les destinataires à qui le responsable de traitement avait communiqué les données en question[111]. Nous n'oublierons pas non plus le droit de s'opposer au traitement de données et le droit de demander la suppression ou la rectification des données traitées[112]. Nous avons déjà évoqué ce point, lorsqu'il est question de quitter le réseau social.

25. Au-delà des règles de protection des données et de manière bien plus générale, l'utilisateur sera tenu de ne pas porter atteinte **à l'honneur et à la considération des personnes**[113]. En matière de calomnie, de diffamation et d'injures, dans la majorité des hypothèses, il sera

(106) Voir *supra* II 3. A.
(107) Voy. notamment l'art. 5 de la LVP.
(108) Voy. art. 12, a), troisième tiret de la directive 95/46. Concernant les possibilités de soumettre une personne à une décision automatisée, voy. l'art. 15 de la directive 95/46.
(109) Voir à ce propos, la Recommandation CM/Rec(2010)13 du Comité des Ministres aux Etats membres sur la protection des personnes à l'égard du traitement automatisé des données à caractère personnel dans le cadre du profilage, adoptée le 23 novembre 2010. A propos de ces pratiques et des risques y liés, J.M. DINANT, C. LAZARO, Y. POULLET et A. ROUVROY, « Profiling and data protection », Report addressed to the Convention 108 consultative Committee, septembre 2008, disponible sur le site du Conseil de l'Europe ; M. HILDEBRANT et S. GUTWIRTH (éds), *Profiling the European Citizen*, Dordrecht, Springer, 2008 ; A. Rouvroy, « Privacy, data protection, and the Unprecedented Challenges of Ambient Intelligence », *Studies in Law, Ethics and Technology*, 2008 et D.HELLMAN, « Classification and fair treatment : an essay on the Moral and Legal Permissibility of Profiling », Univ. of Maryland School of Law, Working Research Paper n° 2003-04, disponible sur www.ssrn.com/abstract=456460.
(110) Voy. les articles 15, § 1er, h), et 20 du projet de règlement.

satisfait à la condition de publicité consacrée dans l'article 444 du Code pénal. Ainsi, l'utilisation d'une fonctionnalité de messagerie instantanée mettant en contact la personne offensée, un témoin et le fautif peut rencontrer cette exigence de publicité. Sans doute, les messages ainsi visés sont protégées par la **confidentialité des communications électroniques, selon l'article 314*bis* du Code pénal**[114] **et donc non accessibles à des tiers non autorisés** mais cette constatation n'empêche pas qu'aux yeux de l'article 344 la communication reste publique. En d'autres termes, un constat de publicité au regard d'une disposition légale (l'article 344 du Code pénal) n'empêche pas que la même situation puisse être couverte par une certaine confidentialité en vertu d'une autre disposition légale (l'article 314*bis* du Code pénal).

26. En matière de **propriété intellectuelle**, il importe de relever que la communication d'œuvres originales dans les réseaux sociaux impliquera souvent une communication au *public* qui excèdera souvent ce *cercle de famille* dans lequel l'auteur perd la maîtrise de son œuvre[115]. Pour faire court, le cercle de mes 130 amis sur Facebook

(111) Dans l'affaire *Rijkeboer* (C.J.C.E. 7 mai 2009 (College van burgemeester en wethouders van *Rotterdam v. M.E.E. Rijkeboer*), aff. C-553/07), la Cour de justice juge que le « droit au respect de la vie privée implique que la personne concernée puisse s'assurer que [...] les données de base la concernant sont [...] adressées à des destinataires autorisés » (point 49) ; « ce droit doit nécessairement concerner le passé » (point 54), même s'il peut être limité dans le temps (doivent être mis en place un accès et un délai qui « constituent un juste équilibre entre, d'une part, l'intérêt de la personne concernée à protéger sa vie privée, notamment au moyen des droits de rectification, d'effacement et de verrouillage des données, en cas de non-conformité du traitement de celles-ci avec la directive, ainsi que des droits d'opposition et d'introduction d'un recours juridictionnel et, d'autre part, la charge que l'obligation de conserver cette information représente pour le responsable du traitement », point 64). Dans ce contexte sont à prendre en compte la nécessité de permettre l'exercice des droits de rectification et d'opposition ainsi que les « obligations, découlant de l'art. 6, sous e), de la directive, [(durée de conservation des données)] » (point 65), et peuvent être considérés « la nature plus ou moins sensible des données de base, la durée de conservation de ces données (« Lorsque la durée de conservation des données de base est très longue, l'intérêt de la personne concernée d'exercer les voies d'intervention et de recours mentionnées au point 57 du présent arrêt, peut, dans certains cas, diminuer », points 58-59) et le nombre des destinataires concernés (Si, par exemple, les destinataires de telles données sont nombreux ou la fréquence de communications à un nombre plus restreint de destinataires est élevée, l'obligation de conserver aussi longtemps l'information sur les destinataires ou les catégories de destinataires ainsi que sur le contenu des données communiquées pourrait représenter une charge excessive pour le responsable du traitement, point 59) » (point 63), ainsi qu'enfin « les risques présentés par le traitement et de la nature des données à protéger, compte tenu de l'état de l'art et des coûts liés à leur mise en œuvre » (points 62-63).
(112) Art. 12 de la Directive 95/46.
(113) Art. 443 et 444 du Code pénal belge.
(114) Qui vise les infractions relatives au secret des communications et des télécommunications privées.
(115) Voy. l'art. 22, § 1er, 3° et 5°, de la LDA. Le cercle de famille est enteudu strictement par la Cour de cassation qui juge par exemple que « la communication privée d'une œuvre musicale qui ne peut être interdite par l'auteur peut consister en la communication gratuite effectuée dans un cercle privé à l'égard de personnes entre lesquelles existe un lien familial, en ce compris un groupe restreint de personnes entre lesquelles existe un lien si étroit qu'il peut être assimilé à un lien familial », Cass. 26 janvier 2006, n° C.05.0219.N. Sur cette exception, F. DE VISSCHER et B. MICHAUX, *o.c.*, pp. 114-115, 143.

ne constitue en principe pas ce cercle familial. On ne peut manquer de rapprocher le concept de « cercle familial », utilisé en droit d'auteur, de celui de d' « activités exclusivement personnelles ou domestiques, sphère domestique et personnelle », prévu par la loi de **protection des données**(116). A nouveau, nous renvoyons à la proposition qui avait été réalisée au Conseil de l'Europe en matière de *household exemption*. Il est piquant de relever ici que ces deux exceptions, l'une à la protection des données, l'autre au droit d'auteur, limitant d'une part, les droits de la personne concernée et d'autre part, ceux de l'auteur, sont précisément motivées par le respect de la vie privée(117).

27. Enfin, il est évident que l'utilisateur entendra empêcher toute usurpation d'identité et éviter qu'un **faux profil** soit ouvert à son nom. Un récent jugement du tribunal correctionnel de Gand considère que l'utilisation d'un faux profil Facebook constitue l'infraction de **faux en informatique**(118). Ce point permet opportunément de passer à cet autre acteur du réseau social que constitue l'entreprise et qui elle aussi luttera contre les faux profils et ainsi une certaine forme de « *cybersquatting* ».

3.2. – *L'entreprise*

28. L'entreprise, en tant qu'opérateur de marché, veille à défendre son image sur le réseau social en se servant, le cas échéant, de son droit à la **marque**(119). Le droit à la marque toutefois, permet de contrôler l'usage d'un signe dans la vie des affaires, il ne permet pas d'étouffer les critiques désagréables que pourraient émettre les consommateurs sur les réseaux sociaux. La présence de l'entreprise dans les réseaux sociaux apparaît aujourd'hui comme nécessaire à sa représentation ; tout le monde y est, probablement doit-elle également y être pour être sûre de bien exister partout où se trouvent les clients potentiels. Ceux-ci pouvant également être atteints par des concurrents le cas échéant aux pratiques illicites – contrefacteurs, trompeurs, etc. – l'entreprise passera du temps à défendre, dans le

(116) Art. 3, § 2 de la loi belge du 8 décembre 1992 déjà citée qui prévoit que la loi ne s'applique pas dans le cas de traitements de ce type. C'est la fameuse « *household exemption* ».
(117) Dans la mesure où le responsable de tels traitements serait obligé de permettre l'accès aux données traitées dans ce cadre, de révéler les finalités poursuivies à titre purement personnel, etc.
(118) Voy. Corr. Gand 21 septembre 2011, *T.Strafr.* 2012, pp. 103-104, note de E. BAEYENS, pp. 104-107, et l'art. 210*bis* du Code pénal.
(119) Voy. la loi uniforme Benelux sur les marques et le Règl. (CE) n° 207/2009 du Conseil du 26 février 2009 sur la marque communautaire, *JO* L. 78, du 24 mars 2009.

contexte des réseaux sociaux, son intégrité, sa réputation et ses **droits de propriété intellectuelle** dont en particulier, son droit d'auteur aujourd'hui particulièrement houspillé dans le contexte audiovisuel – *e.g.* YouTube, les forums de partage de liens de *direct download*, etc. –, à moins qu'il ne s'agisse avec les mouvements *d'open source* ou d'*open document*, fort prisés par les jeunes générations, d'une simple renonciation aux droits patrimoniaux d'auteur mais certes non aux droits moraux et en particulier au droit à la paternité.

29. C'est bien entendu également pour des raisons de **publicité** que l'entreprise utilise le réseau social et les fonctionnalités publicitaires qu'il offre, telles que la publicité ciblée basée sur un profilage paramétré par l'entreprise elle-même(120). A ce propos, lorsqu'une entreprise décide d'utiliser un réseau social et les fonctionnalités de publicité ciblée offertes, afin d'atteindre une audience bien spécifique selon des critères plus ou moins précis (âge, sexe, lieu de résidence, centres d'intérêt, mots-clés, etc.), nous nous demanderons s'il est possible de la considérer comme co-responsable, avec le fournisseur du réseau social, du traitement de données à caractère personnel ainsi réalisé(121). Cela quand bien même aucune donnée à caractère personnel ne lui serait communiquée. Probablement est-ce aller trop loin ! Pourtant, sans les entreprises, des fonctionnalités de publicité ciblée telles que celles offertes par Facebook ne seraient pas utilisées et ne donneraient donc lieu à aucun traitement de données. Ont-elles une responsabilité particulière à cet égard ? Les pratiques du commerce, plus récemment appelées **pratiques du marché**, intéresseront plus directement l'entreprise soucieuse de licitement réaliser la publicité de ses biens et produits. On pense ici à toutes les nouvelles techniques de publicité susceptibles d'être mises en œuvre au-delà de la problématique classique des communications non sollicitées(122). Par exemple, il est imaginable qu'une entreprise de prêt à porter conçoive une application Facebook permettant à tout utilisateur, à partir de sa photo, d'essayer des vêtements.

Ceci permet, en passant, de souligner l'importance des développeurs d'application en matière de réseaux sociaux. Ces applica-

(120) A ce propos, lire le rapport de la FTC, « *Protecting Consumer Privacy in an Era of Rapid Change : A proposed Framework for Businesses and Policy makers* », 1er décembre 2010 disponible sur www.ftc.gov/os/2010/12/101201privacyreport.pdf.
(121) A ce propos, voy. J.-P. MOINY, « Facebook au regard des règles européennes de protection des données », *REDC* 2010/2, pp. 254-255.
(122) Voy. C. COLIN et Y. POULLET, « Du consommateur et de sa protection face à de nouvelles applications des technologies de l'information : risques et opportunités », *DCCR* 2010, n° 88, pp. 94-145.

tions constituent souvent un moyen de collecte – traitement – de données à caractère personnel. Dans l'industrie mobile, la quantité d'applications disponibles est d'ailleurs un des éléments qui, nous n'en douterons pas, est de nature à conduire le consommateur vers l'une ou l'autre plateforme logicielle – Androïd ou Mac.

30. En tant qu'**employeur**, l'entreprise voudra aussi contrôler l'utilisation des réseaux sociaux mais cela d'une façon assez différente de celle déjà évoquée. D'une part, l'on pense bien entendu au **contrôle du l'utilisation des TIC sur le lieu du travail**[123]. Et d'autre part, il est question du licenciement pour motif grave en raison de propos tenus dans les réseaux sociaux. A nouveau malheureusement, nous ne sommes ici pas exhaustifs[124]. Quant à la première problématique, on sait bien que la Cour européenne des droits de l'homme a reconnu de manière édifiante dans l'affaire *Niemietz c/ Allemagne* que le droit à la vie privée du travailleur ne s'arrêtait pas aux portes de l'entreprise : en ce sens la « Cour ne juge ni possible ni nécessaire de chercher à définir de manière exhaustive la notion de « vie privée« . Il serait toutefois trop restrictif de la limiter à un « cercle intime« où chacun peut mener sa vie personnelle à sa guise et d'en écarter entièrement le monde extérieur à ce cercle. Le respect de la vie privée doit aussi englober, dans une certaine mesure, le droit pour l'individu de nouer et développer des relations avec ses semblables. Il paraît, en outre, n'y avoir aucune raison de principe de considérer cette manière de comprendre la notion de « vie privée » comme excluant les activités professionnelles ou commerciales : après tout, c'est dans leur travail que la majorité des gens ont beaucoup, voire le maximum d'occasions de resserrer leurs liens avec le monde extérieur »[125]. Toutefois, l'employeur demeure libre, au titre de son droit de propriété ou plus simplement de son droit de contrôler l'activité de ses employés, de définir l'usage autorisé des TIC mises à disposition du travailleur. Il peut donc interdire l'accès aux réseaux sociaux via les outils qu'il met à disposition du travailleur. Toutefois s'il l'autorise explicitement ou implicitement dans une certaine mesure, ce qui tend à se généraliser, il va de soi qu'il n'obtient pas en conséquence un droit de regard sur

(123) A ce sujet, voy. la récente Recommandation n° 08/2012 (12 mai 2012) de la CPVP relative au contrôle de l'employer de l'utilisation des outils de communication électronique sur le lieu du travail. Pour plus de détails R. ROBERT et K. ROSIER, « Réglementation et contrôle de l'utilisation des technologies de la communication et de l'information sur le lieu du travail » in *Le droit du travail à l'ère du numérique, Les technologies de l'information et de la communication dans les relations de travail*, K. ROSIER (éd.), Anthemis, 2011, pp. 231-359.

(124) Par exemple, *quid* de l'utilisation des réseaux sociaux en matière de recrutement ?

(125) CEDH 16 décembre 1992, arrêt *Niemietz v. Allemagne*, req. n° 13710/88, § 29.

le profil et l'activité de son travailleur. Le propos touche ici au contrôle de l'utilisation des TIC par les travailleurs, contrôle déjà strictement encadré, entre autres par la convention collective de travail n° 81[126].

31. Quant à la seconde problématique, celle du **licenciement** pour propos tenus sur les réseaux sociaux, on retiendra que si l'employeur a licitement accès à ces propos – *e.g.* le profil est ouvert ou quelqu'un rapporte l'information à l'employeur (avec toutefois le risque que cette communication d'information soit elle-même illicite[127]) – un fait de la vie privée peut être constitutif d'un motif grave[128]. La difficulté consistera dans la preuve de ce motif grave et c'est surtout sa licéité qui sera débattue. Aujourd'hui, plusieurs arrêts de la Cour de cassation tendent à démontrer, à tout le moins en procédure pénale, que le respect de la loi vie privée n'étant pas prescrit à peine de nullité, sa violation n'emporte pas l'irrégularité de la preuve ; il incombe au juge d'exercer à ce sujet son pouvoir d'appréciation – nous y venons juste *infra*[129]. On a ici envie de conclure un peu péremptoirement que ce qui vaudra en droit pénal, lieu du respect le plus strict des droits de la défense et du prévenu – devrait valoir *a fortiori* en droit civil. Ces considérations permettent passer à un utilisateur moins visible du réseau social : l'autorité publique.

3.3. – *Les autorités publiques*

32. L'autorité publique entend également utiliser les réseaux sociaux. Rappelons-le encore une fois, nous ne serons pas exhaustifs. Le fisc peut servir d'exemple. En matière de fiscalité, on pense ici au nouveau BISC – Belgian Internet Service Center[130] qui contrôle et surveille l'activité fiscalement taxable et non déclarée des citoyens sur

(126) Convention collective du travail n° 81 relative à la protection de la vie privée des travailleurs à l'égard du contrôle des communications électroniques en réseau, Convention rendue obligatoire par arrêté royal du 12 juin 2002.

(127) Lorsque le profil est par exemple fermé et qu'un utilisateur qui a accès à ce profil utilise ses droits d'accès pour ensuite communiquer l'information à l'employeur de la personne concernée, il réalise un traitement de données à caractère personnel au sens de la LVP.

(128) Pour un cas où le motif grave n'est pas retenu, voy. par exemple Cour du travail de Bruxelles (2e ch.) 4 mars 2010, *RDTI* 2010, n° 46, vol. 1, pp. 73 et s. Au sujet du motif grave et de sa preuve, voy. S. GILSON, K. ROSIER, A. FRANKART et M. GLORIEUX, « La preuve du motif grave » in *Le congé pour motif grave, Notion, évolutions, questions spéciales*, S. GILSON (coord.), Anthemis, 2011, pp. 169-250.

(129) Voy. *infra*, n^{os} 34 et s.

(130) Voy. www.belgium.be/fr/actualites/2011/news_bisc.jsp.

les réseaux afin de percevoir le juste impôt. Evidemment, certains réseaux sociaux attireront plus son attention que d'autres. On pense à des sites tels que 2ememain.be ou eBay – mais également Facebook qui a déjà permis la vente de biens via la fonctionnalité Marketplace. Il est évident que l'utilisateur de tels réseaux est susceptible d'y mener – et si facilement – une véritable activité commerciale de ventes et d'achats de bien, le cas échéant sans déclarer ses revenus et en fraudant donc la réglementation fiscale voire également, la réglementation du chômage. Le service public est ici susceptible d'utiliser les réseaux sociaux pour enrichir ses bases de données et mener ses enquêtes, ce qui fait bien entendu de lui un responsable de traitement au regard de la loi vie privée.

33. De manière plus générale, la lutte contre la fraude sur Internet – que celle-ci concerne le fisc[131], la vente de biens contrefaits (en particulier, les médicaments), etc. – et la lutte contre la cybercriminalité ou encore la criminalité « traditionnelle » si l'on peut dire, passe également par l'utilisation des réseaux sociaux par la police et le ministère public[132]. Le réseau social peut en dire bien plus qu'une caméra de surveillance. Pensons par exemple à une application telle que Google Latitude qui permet de savoir où se trouvent les contacts d'un utilisateur[133]. Alors d'une part, la police peut elle-même tenter d'extraire des informations du réseau social, ou encore en recevoir des victimes, et se posera alors à nouveau la question de la recevabilité de

(131) A cet égard, le fisc souhaiterait à l'instar de la police être exempté de certaines obligations nées de la loi de protection des données, en particulier des obligations d'information et d'accès lors de l'instruction des dossiers. La récente loi du 3 août 2012 portant dispositions relatives aux traitements de données à caractère personnel réalisés par le Service public fédéral Finances dans le cadre de ses missions (*MB* 24 août 2012) vient de leur accorder cette exemption par l'ajout à la liste des autorités exemptées des articles 9, 10, § 1er (obligation d'information), et 12 (droit d'accès des personnes concernées). La loi fait actuellement l'objet d'un recours à la Cour constitutionnelle. A cet égard, on note le communiqué de la CPVP indigné de voir son avis négatif non suivi par le législateur : « Le 24 août dernier, une nouvelle loi a été publiée au Moniteur belge concernant le traitement de données à caractère personnel par le Service public fédéral Finances. Comme toujours lorsqu'une loi concerne le traitement de données à caractère personnel, le projet de texte a d'abord été soumis à l'avis de la Commission vie privée. Cet avis était favorable dans ce cas-ci, moyennant la prise en compte d'un certain nombre de remarques. La principale inquiétude portait sur le manque de précision concernant l'accès des citoyens à leurs données dans la banque de données du fisc. Lors de la publication du texte au Moniteur belge, il est apparu que les remarques de la Commission vie privée n'ont finalement pas été intégrées, pire encore, que le texte a même été modifié, dans le mauvais sens, par rapport au document qui avait été soumis pour avis. »

(132) Sur l'utilisation par les autorités policières et judiciaires dans le cadre de procédures civiles ou pénales, lire le relevé de cas mentionnés par l'article « *Use of social network websites in investigations* », publié sur Wikipedia, disponible sur http://en.wikipedia.org/wiki/Use_of_social_network_websites_in_investigations, le 17 septembre. Voy. un sondage réalisé en ligne par LexisNexis sur cette question, « Role of Social Media in Law Enforcement Significant and Growing », 18 juillet 2012, au sujet duquel les liens suivants peuvent être consultés : www.lexisnexis.com/risk/newsevents/press-release.aspx?id=1342623085481181 ; www.lexisnexis.com/government/investigations/.

(133) Voy. www.google.com/mobile/latitude/.

la preuve devant les juridictions répressives[134]. Parmi une jurisprudence abondante, nous n'évoquerons ici que deux décisions. D'abord l'arrêt dit *Antigone*[135], à l'origine d'un tournant – « une révolution »[136] – dans la recevabilité des preuves en matière pénale en général ; à « une interdiction de principe de l'utilisation des preuves illicites, [la Cour de cassation] a substitué une autorisation de principe, sauf dans trois cas précis »[137] ; d'après la Cour : « soit lorsque le respect de certaines conditions de forme est prescrit à peine de nullité ; soit lorsque l'irrégularité commise a entaché la fiabilité de la preuve ; soit lorsque l'usage de la preuve est contraire au droit à un procès équitable » ; une preuve obtenue en méconnaissance d'un droit fondamental garanti par la CEDH ou la Constitution *n'est pas* « à jamais inadmissible ». Cette jurisprudence, qui a pu être critiquée par les pénalistes, a en tous cas été entérinée par la jurisprudence de la Cour EDH[138] qui juge qu'un procès peut être équitable au sens de l'article 6 CEDH malgré une violation de l'article 8 CEDH. En comparaison aux Etats-Unis, quoique nous ayons pu identifier certaines imperfections dans la consécration du *right to privacy*[139], lorsque le *Fourth Amendment* est violé, c'est en tous cas toute la procédure qui tombe à l'eau, comme vient encore de récemment l'illustrer l'utilisation illicite, par la police, d'un dispositif GPS caché sur le véhicule d'une personne suspectée de trafic de stupéfiants[140].

Quoi qu'il en soit, la jurisprudence Antigone vaut aujourd'hui assez largement en Belgique et d'ailleurs à sa suite, l'arrêt dit *Manon*[141], qui concerna plus directement la vie privée et la protection des données, la confirme. Dans cette affaire, une employée avait été licenciée sur la base d'une vidéosurveillance exercée, alléguait à juste titre la requérante, en violation de la CCT n° 68. L'employeur avait violé son obligation d'information en taisant l'existence de cette méthode de surveillance. La Cour, relève que l'éventuelle violation de la CCT par l'employeur n'est pas sanctionnée de nullité par la loi, et ajoute que « lorsque l'irrégularité ne compromet pas le droit à un procès équitable, n'entache pas la fiabilité de la preuve et ne méconnaît pas une formalité prescrite à peine de nullité, le juge peut, pour décider qu'il y a

(134) Déjà évoquée *supra*, au n° 32.

(135) Cass. (2e ch.) 14 octobre 2003, R.G. n° P.03.0762.N.

(136) H.D. BOSLY, D. VANDERMEERSCH et M.-A. BEERNAERT, *Droit de la procédure pénale*, La Charte, 2010, p. 1010.

(137) *Ibid.*

(138) CEDH 28 juillet 2009, arrêt *Lee Davies v. Belgique*, req. n° 18704/05/74.

(139) Et par la même occasion, pointer des solutions propres à ce droit, voy. J.-P. MOINY, « Cloud Based Social Network Sites : Under Whose Control ? », *o.c.*, pp. 157-161.

(140) Voy. Supreme Court of the United States, *United States v. Jones*, 23 janvier 2012.

(141) Cass. (2e ch.) 2 mars 2005, R.G. n° P.04.1644.F. Voir également.

lieu d'admettre des éléments irrégulièrement produits, prendre en considération, notamment, la circonstance que l'illicéité commise est sans commune mesure avec la gravité de l'infraction dont l'acte irrégulier a permis la constatation, ou que cette irrégularité est sans incidence sur le droit ou la liberté protégés par la norme transgressée ». Selon la Cour, une telle hypothèse se vérifie aussi en cas de violation des règles légales de protection des données. La Cour de cassation autorise dès lors *in fine* la violation de LVP dans l'obtention de la preuve, certes sous conditions et après analyse par le juge du fond des critères rappelés ci-dessus. Cette jurisprudence hardie semble *a priori* fortement diminuer la force obligatoire des règles de protection des données et donc déforce substantiellement ces dernières. Nous venons de rappeler, aux Etats-Unis, avec quelle sévérité sont sanctionnées les violations du *fourth amendment* dans les procédures pénales. Cependant *a posteriori*, eu égard à la complexité de l'interprétation et de l'application de la LVP, dans le contexte changeant des nouvelles technologies, ne peut-on estimer que la Cour de cassation ait voulu ménager aux juges du fond une telle souplesse qui, il faut le dire, peut parfois véritablement être salutaire. Cette jurisprudence, sans évidemment ôter le pouvoir du législateur de reprendre la main et de prescrire à peine de nullité la violation de la loi de protection des données, permet, on le conçoit, d'éviter une annulation de procédure qui conduirait à un sentiment profond d'injustice, voire qui discréditerait la justice. Certes, le tout est dans la mesure et l'essentiel sera d'être sévère dans l'analyse des critères fournis par la Cour de cassation, sous peine d'amoindrir significativement et de manière disproportionnée l'effectivité des règles de protection des données.

34. D'autre part, le ministère public peut encore solliciter la **collaboration** *volontaire* du fournisseur du réseau social, ou le *contraindre*, en vertu de ses pouvoirs, à communiquer des informations d'identification. Nous ne nous attarderons pas sur la possibilité de collaboration volontaire d'un intermédiaire tel que le fournisseur de réseau social, même s'il est clair qu'aujourd'hui, la collaboration des entreprises fournissant des services en ligne – du fournisseur d'accès à Internet au fournisseur de boîtes mail – est un élément important en matière de lutte contre la cybercriminalité[142]. Notons juste que s'il est question de communication volontaire de données à caractère personnel à des autorités publiques, l'entreprise concernée devrait être alors qualifiable de responsable – ou coresponsable – de ce traitement de communication de données. Il en va autrement lorsque sa collaboration est « enjointe » par la loi et le ministère public. On relèvera ici une question d'actualité juridique belge relative à l'article 46*bis* du CIC et à la définition de fournisseur de service de communications électroniques[143]. Une affaire récente concernait la société américaine Yahoo!, le ministère public entendant obtenir de Yahoo!, en application de l'article 46*bis* du CIC, des données d'identification d'utilisateurs de boîtes *email*[144]. La Cour de cassation a finalement, à cette occasion, été saisie de la question de savoir si la disposition précitée du CIC consacrait ou non le même concept fournisseur de services de communications électroniques (ou fournisseur de réseau) que celui consacré dans la LCE. La Cour, cassant la Cour d'appel qui selon nous, avait jugé à bon droit que Yahoo! n'était pas un fournisseur de service de communications électroniques au sens de la LCE *et par conséquent* du CIC[145], considère que les concepts utilisés dans les deux textes légaux sont différents. Il s'agit là d'une application du principe d'autonomie du droit pénal, même si celle-ci s'exerce aux dépens de la prévisibilité du texte. Ce concept de service de communication électronique est en effet au cœur de l'arsenal législatif européen en matière de communications électroniques ; il est un des concepts centraux de la directive « cadre » du droit européen des communications électroniques[146]. Il y est d'ailleurs à nouveau fait référence, dans la *data retention directive*, lorsqu'il est question, pour leurs fournisseurs ou les fournisseurs de réseaux publics de communications électroniques, de conserver les données de connexions des abonnés[147]. L'affaire précitée

(142) Cela a encore été vivement rappelé à l'occasion de la dernière conférence Octopus, sur la cybercriminalité, organisée par le Conseil de l'Europe (Voy. le workshop 2, « Public/Private Information Sharing, www.coe.int/t/DGHL/cooperation/economiccrime/cybercrime/cy_Octopus2012/2571_octo12_outline_v4_22Mar12.pdf, consulté le 17 septembre 2012).

(143) L'art. 46*bis* du CIC stipule que « § 1er. [...] le procureur du Roi peut, [...] en requérant au besoin le concours de l'opérateur d'une réseau de communicatiou électronique ou d'un fournisseur d'un service de communication électronique [...], procéder ou faire procéder sur la base de toutes données détenues par lui, ou au moyen d'un accès aux fichiers des clients de l'opérateur ou du fournisseur de service à : 1° l'identification de l'abonné ou de l'utilisateur habitnel d'un service de communication électronique ou du moyen de communication électronique utilisé ; 2° l'identification des services de communication électronique auxquels une personne déterminée est abonnée ou qui sont habituellement utilisés par une personne déterminée. [...] ».

(144) Corr. Termonde 2 mars 2009, *T.Straf.*, 2009, pp. 116-124. Sur le point de la qualification de fournisseur de service de communications électroniques, la décision du tribunal a été réformée par un arrêt du 30 juin 2010 de la Cour d'appel de Gand (disponible sur jure.juridat.just.fgov.be/view_decision?justel=N-20100630-1&idxc_id=242315&lang=fr), qui a lui-même été cassé par la Cour de cassation (Cass. (2e ch.) 18 janvier 2011, *RDTI* 3/2011, pp. 114-115 et note de L. KERZMANN, pp. 116-123).

(145) Les termes du CIC avait été aligné sur la LCE, voy. Amendement n° 1 du Gouvernement au Projet de loi modifiant l'art. 46*bis* du Code d'instruction criminelle, *Doc. Parl.* Sénat sess. 2006-07, n° 3-1824, 11 octobre 2006, pp. 1-2. Le concept antérieur (« fournisseur d'un service de télécommunication ») apparaissait encore plus restrictif quant aux vocables choisis.

(146) Voy. *supra*, note de bas de page n° 82.

(147) Dir. (CE) n°2006/24 du Parlement européen et du Conseil du 15 mars 2006 sur la conservation de données générées ou traitées dans le cadre de la fourniture de services de communications électroniques accessibles au public ou de réseaux publics de communications, et modifiant la directive 2002/58/CE, *JO* L. 281, du 13 avril 2006.

peut illustrer deux choses. D'une part, existent encore récemment, malgré la pénétration toujours plus grande dans la société des réseaux sociaux et des TIC, des difficultés d'interprétation substantielles des dispositions légales rencontrées par les hautes juridictions en matière de droit des nouvelles technologies ou plutôt de droit de l'Internet. D'autre part, la décision de la Cour de cassation se comprend également parfaitement d'un point de vue politique et pratique. Il est certainement souhaitable aujourd'hui que des prestataires tels que Yahoo! et Google puissent être contraints de collaborer à l'identification des prévenus d'infractions graves.

3.4. – *Le fournisseur du réseau social*

35. Le fournisseur du réseau social, lance son entreprise, il est peut-être seul ou avec un associé et dispose de peu de moyens, et il veut maîtriser les risques notamment juridiques de son projet informatique. Sa première préoccupation concernera sa propre responsabilité au cas où un utilisateur via ou grâce à son réseau se livre à des opérations dommageables pour des tiers ou dont l'illicéité est dénoncée. Ainsi, un internaute met à disposition de ses amis une copie de film sans autorisation de l'auteur, diffuse des propos racistes ou des images de tiers sans leur consentement. La victime de tels agissements peut se retourner vers l'opérateur du réseau et lui enjoindre de prendre les mesures qui s'imposent voire recourir à la justice face à un opérateur qui « aurait dû intervenir ».

36. L'articulation des alinéas 1 et 2 de l'article 10 CEDH est particulièrement malaisée dans le contexte des technologies nouvelles pour diverses raisons. L'utilisation de mesures techniques comme le filtrage du contenu, le blocage en ligne de certains contenus[148] est tentante tant de la part des pouvoirs publics qui pourrait appliquer de manière disproportionnée et trop large des lois comme celles sur la diffamation, l'injure, la lutte antiterroriste, etc., mais également pour les pouvoirs privés. A cet égard, l'Assemblée parlementaire du Conseil de l'Europe affirme : « ce sont principalement des intermédiaires privés qui déterminent l'accès des particuliers et du grand

(148) Sur l'équilibre entre liberté d'expression et mesures de filtrage, lire la Recommandation CM/Rec(2008)6 du Comité des Ministres aux Etats membres, sur les mesures visant à promouvoir le respect de la liberté d'expression et d'information au regard des filtres Internet. Lire également le « Rapport du Groupe de spécialistes sur les droits de l'homme dans la société de l'information (MC S IS) sur l'utilisation et l'impact des mesures de filtrage technique pour divers types de contenus dans l'environnement numérique », CM(2008)37.

public à des services médiatiques fondés sur les TIC. Nombre de ces intermédiaires [...]ont une position dominante vis-à-vis des utilisateurs parce qu'ils ont une importance significative pour le système ou qu'ils exercent une emprise considérable sur le marché »[149]. Au nombre de ces intermédiaires en position monopolistique ou quasi-monopolistique, il faut compter certains fournisseurs de réseaux sociaux et on connaît certaines pratiques de ces entreprises limitatrices des libertés, tantôt au service d'une autorité publique peu démocratique, tantôt au service de leurs propres intérêts commerciaux.

Sans doute cette pratique peut s'expliquer par la crainte des opérateurs de réseaux sociaux de voir leur responsabilité engagée du fait des contenus circulant sur le Net ou des pratiques illégales de certains de leurs sous-traitants. Quand bien même toutefois, un discours, par exemple, serait permis dans un Etat, le fournisseur du réseau social pourrait souhaiter l'interdire de manière globale pour éviter tout litige. Une autre affaire Yahoo!, plus ancienne[150] celle-là, concernait cette fois la mise en vente d'objets nazis sur un site américain, ce qui était licite outre atlantique mais ne l'était point en France. Yahoo! fut condamné en France pour avoir permis cette diffusion sans avoir bloqué l'accès des internautes français au site incriminé. Nous pensons ici aux limites que l'offreur du réseau social pourrait souhaiter imposer à la liberté d'expression de ses utilisateurs, le cas échéant via des logiciels de filtrage. L'existence de ces logiciels acceptée par les internautes soulève la question de la renonciation aux droits fondamentaux et celle de l'effet horizontal de ceux-ci. Contractuellement, jusqu'où le prestataire de service peut-il obtenir consentement à une limitation des droits fondamentaux des utilisateurs? Il peut être tenté d'empêcher l'accès à son réseau pour ceux qui tiennent des propos qui dérangent. Dès lors que le réseau social devient un véritable espace public de discussion, jusqu'où peut aller le réseau social à cet égard ; est-il tenu à la pluralité ?

(149) Résolution 1877 (2012) de l'Assemblée parlementaire du Conseil de l'Europe adoptée le 25 avril 2012, *o.c.* point 9.

(150) A propos de cette affaire, voy. B. DE GROOTE, avec la collaboration de J.-F. DERROITTE, « L'Internet et le droit international privé : un mariage boiteux ? A propos des affaires Yahoo! et Gutnick », *Revue Ubiquité* 2003/16, pp. 62-68. En substance, la vente d'objets nazis via le site d'enchère de Yahoo! et la diffusion, via des sites hébergés par un service de Yahoo!, d'extraits de Mein Kampf étaient critiquées notamment par la LICRA en raison de la violation de la loi française qui en résultait. Il fut ordonné à Yahoo! de filtrer l'accès aux sites et pages en question, de telle sorte que les internautes français ne puissent plus y accéder. Les différentes décisions françaises sont disponibles sur www.juriscom.net/txt/jurisfr/cti/tgiparis20001120.htm.

37. Cette problématique renvoie à la vaste jurisprudence – française surtout – concernant les **intermédiaires d'Internet**[151]. Des réseaux sociaux tels que YouTube et Dailymotion peuvent-ils bénéficier de l'exonération de responsabilité applicable aux hébergeurs quant au contenu hébergé ? La jurisprudence, en particulier en France, a tergiversé. Sans approfondir le sujet, il n'est pas toujours évident de qualifier la plupart de ces opérateurs de simples hébergeurs au sens de l'article 14 de la directive européenne dite *e-commerce*[152]. Ces derniers sont exonérés selon l'article 15 de la directive, de tout devoir de surveillance générale et tenus à agir uniquement en cas de connaissance de l'illégalité commise. Les multiples services offerts par les opérateurs y compris d'analyse des contenus (par exemple reconnaissance faciale ou publicité appropriée en fonction des contenus de messages envoyés ou des destinataires des messages) posent la question du rôle de ces opérateurs vis-à-vis des contenus qu'ils hébergent. L'activité du prestataire du réseau social est-elle « purement technique, automatique et passi[ve] »[153] ? Comme la Cour de justice l'a récemment jugé, afin d'évaluer la responsabilité du prestataire de service, « il convient d'examiner si le rôle exercé par le dit prestataire est neutre, en ce que son comportement est purement technique, automatique et passif, impliquant l'absence *de connaissance ou de contrôle des données qu'il stocke* »[154] (italique ajouté par nous). Ne conviendrait-il pas ici d'établir au cas par cas et *selon les fonctionnalités offertes*, certes automatisées, si ces dernières sont de nature à conférer une connaissance du *contenu litigieux* du réseau social ou un contrôle sur celui-ci à son prestataire ? D'après l'article 14, il ne faut pas que le prestataire de service ait une connaissance *effective* de l'information ou de l'activité illicites. Dans le contexte des réseaux sociaux, c'est probablement cet élément de connaissance effective qui fera débat dans la mesure où le prestataire de service, à tout le moins en ce qui concerne les profils des utilisateurs « de base », ne contrôle pas le contenu qu'ils diffusent – instantanément, chacun est techniquement libre du diffuser du contenu (le cas échéant contraire

(151) Lire en particulier, sur cette jurisprudence, E. MONTERO, Les responsabilités liées au Web 2.0, *RDTI* 2011, pp. 363 et s., et l'art. plus récent de R. HARDOUIN, « La connaissance de l'illicéité par les hébergeurs ou quand être notifié ne signifie pas nécessairement devoir retirer », *RDTI* 2012, pp. 5 et s.
(152) Dir. (CE) no 2000/31 du Parlement européen et du Conseil du 8 juin 2000, relative à certains aspects juridiques des services de la société de l'information, et notamment du commerce électronique, dans le marché intérieur, *JO* L. 178 du 17 juillet 2000.
(153) Considérant n° 42 de la directive *e-commerce*.
(154) C.J.U.E. 23 mars 2010 (*Google France v. Louis Vuitton et al.*), affs C-236/08 à C-238/08, point 114. Dans cette affaire mettant en cause la célèbre fonctionnalité AdWords de Google, la Cour relève qu'est pertinent dans cette analyse « le rôle joué par Google dans la rédaction du message commercial accompagnant le lien promotionnel ou dans l'établissement ou la sélection des mots clés », point 118.

aux conditions d'utilisation). Nous l'avons évoqué, peuvent exister des fonctionnalités d'analyse du contenu, en particulier pour des finalités « one to one marketing ». Dans ce cas, la connaissance *quant au contenu* qui *résulte de cette analyse* – critères utilisés, résultats obtenus – réalisée *pour son compte*, si elle révèle un fait ou une activité illicite, pourrait faire perdre au prestataire de service le bénéfice de l'exonération de responsabilité quant au dommage causé par ce contenu. En effet là, ne pourrions-nous pas considérer qu'il y a connaissance effective de la part du prestataire ? Par contre, lorsque l'utilisateur « de base » diffuse un contenu au travers du réseau, le fournisseur du réseau social n'a en principe pas connaissance effective de celui-ci et ne le contrôle pas[155]. Ainsi, Facebook ne devrait pas être tenu pour responsable de la publication d'informations diffamantes par un utilisateur, etc. Sauf au cas où informée de manière circonstanciée de cette situation, la société n'aurait pas promptement réagi[156]. La situation est toutefois plus complexe lorsque la fonctionnalité d'analyse de contenu en question est mise au service d'un tiers. En effet dans ce cas, l'utilisation de la fonctionnalité ne donne en principe aucune connaissance effective au prestataire du réseau social. Prenons l'exemple de Facebook. Des pages peuvent être dédiées à des entreprises. Lorsqu'un utilisateur enregistre ainsi une entreprise – une marque – Facebook a une connaissance effective de l'utilisation par celui-là du signe représentant la marque. Nous n'en avons pas la place ici mais la fonctionnalité de publicité ciblée de Facebook pourrait être analysée au regard de la jurisprudence précitée de la Cour de justice quant au service Google AdWords.

On évoquera enfin, en renvoyant à l'affaire *Scarlet* soumise à la CJUE[157] en matière de filtrage, une décision anciennement fort contestable, et finalement condamnée par la Cour de justice, du tribunal de première instance de Bruxelles qui avait imposé à Scarlet –

(155) Il est toutefois vrai que juridiquement, via les conditions d'utilisation – le contrat –, le prestataire de service entendra encadrer le comportement de ses utilisateurs pour qu'à tout le moins, il soit conforme à la loi. Cette tentative de « contrôle juridique », si l'on peut dire, des contenus communiqués, lorsqu'elle n'est pas accompagnée d'un contrôle *systématique in concreto* (ou *de facto*, par exemple via des logiciels d'application systématique), ne pourrait-elle être considérée comme *ne* constituant *pas* ce contrôle du contenu qui ferait perdre au prestataire le bénéfice de l'exonération de responsabilité ? L'objectif poursuivi ici par le prestataire est de limiter sa responsabilité juridique personnelle. Ôterait-on à un fournisseur d'bébergement « classique » – offrant de l'espace pour héberger un site Web par exemple – le bénéfice de l'exonération de responsabilité au motif que ses conditions d'utilisation entendent contrôler le contenu en ce qu'elles l'imposent *licite au regard du droit* ? Assurément, nous ne le pensons pas. *Quid* toutefois lorsque le prestataire entend réaliser, et s'en réserver le droit, des contrôles *occasionnels* des contenus ? Dans ce cas alors, seul le contenu effectivement contrôlé devrait pouvoir être considéré comme étant effectivement connu.
(156) Art. 14, § 1, b) de la directive *e-commerce*.
(157) C.J.U.E. (3e ch.) 24 novembre 2011 (*Scarlet Extended v. SABAM*), aff. C-70/10.

un fournisseur d'accès à Internet – une obligation de filtrage des communications électroniques clairement équivalente à une obligation générale de surveillance du trafic Internet passant par son intermédiaire.

38. Il est clair que face à des problèmes éventuellement complexes de responsabilité, le fournisseur du réseau social tentera de limiter contractuellement sa responsabilité – il ne le pourra à l'égard de la LVP qui est d'ordre public. Il s'agit là d'un premier élément d'une sorte de **triptyque contractuel** par lequel il tentera de limiter ses risques – triptyque somme toute classique quant aux services en ligne : des clauses de limitation ou d'exonération de responsabilité, des clauses de modification ou de résolution unilatérales du contrat et enfin, des clauses relatives au droit international privé (choix du droit applicable et du juge ou de l'arbitre compétent). Sans entrer dans les détails, on relèvera que le fournisseur du réseau social tentera de désigner le droit applicable à l'ensemble des relations juridiques existant entre lui et ses utilisateurs. Par la même occasion, il ne se privera pas de choisir le juge compétent pour trancher les éventuels litiges. Dans un contexte de réseaux à utilisation de plus en plus internationale, ce qu'accroît encore le phénomène du « *cloud computing* » et l'omniprésence des sociétés américaines dans l'offre des services, ce type de choix risque de rendre peu effectives les protections multiples proposées par notre droit sinon belge du moins européen. Néanmoins, de telles clauses connaissent, en droit de la consommation et en droit international privé des limites bien connues vis-à-vis des consommateurs[158] – et donc pas des professionnels qui devront tenter de négocier même si souvent eux aussi, adhèrent. Au-delà, on ajoute que la LVP, qui est une loi d'application immédiate et dont l'article 3*bis* définit impérativement le champ d'application spatial, ne pourra subir l'influence d'un tel choix de loi[159]. Enfin, soucieux de maîtriser son réseau, ses fonctionnalités et finalités, le fournisseur du réseau social entendra, via des clauses contractuelles de modification unilatérale ou en tous cas, « quasi-unilatérales »[160], s'en donner le pouvoir juridique – contractuel. Cette unilatéralité ou « quasi-unilatéralité » a déjà été évoquée, en particulier quant à ses limites en matière de protection des données. Le fournisseur du réseau se donnera également aussi le droit d'exclure des participants de son réseau social, ou de mettre un terme à l'utilisation d'un profil – clause de résolution unilatérale.

(158) Voy. en détails à ce sujet J.-P. MOINY et B. DE GROOTE, « 'Cyberconsommation' et droit international privé », *RDTI* 37/2009, pp. 5-37.
(159) Voy. à ce sujet J.-P. MOINY, « Facebook au regard des règles européennes de protection des données », *o.c.*, pp. 255-264 et 267-270.
(160) La poursuite de l'utilisation du site, après modification, étant réputée exprimer le consentement de l'utilisateur, il est difficile de considérer que la modification qui va prendre cours est purement unilatérale – elle semble bilatérale, du moins sur le papier. Mais concrètement, il s'agira souvent d'une modification unilatérale des conditions d'utilisation.

4. – CONCLUSIONS

39. La palette des réseaux sociaux est large et tout autant celle des questions juridiques soulevées par ces réseaux. Pas étonnant vu la diversité des usages de ces réseaux qui de plus en plus collent à la vie des citoyens, les accompagnent dans leurs déplacements et émotions et deviennent pour chacun d'entre nous un second eux-mêmes. Toutes les branches du droit se voient interrogées. Au-delà de ce constat, le droit se voit confronté à un certain malaise. Ce malaise n'est pas sans créer une certaine insécurité juridique. Pour les acteurs de terrain, la première cause du malaise naît sans doute de la difficulté liée à la compréhension de certains concepts fondamentaux du droit applicable aux réseaux sociaux. Tantôt ils reçoivent à l'occasion du développement des réseaux sociaux et de l'Internet en général une signification nouvelle ainsi, pour ne reprendre des exemples qu'en matière de protection des données, la notion de donnée à caractère personnel, la définition du flux transfrontière de données et de l'activité exclusivement personnelle ou domestique. Tantôt l'accumulation des réglementations spécifiques multiplient l'utilisation de concepts aux contours flous qui peuvent, le cas échéant, se superposer, ainsi l'opérateur d'un réseau est à la fois qualifiable de fournisseur de service de communications électroniques, de prestataire de service de communication électronique, d'hébergeur, de responsable de traitement,... Le consentement devient un concept à géométrie variable lorsqu'il s'agit de passer du droit à l'image, du droit à la protection des données ou du droit des contrats électroniques. Ces divergences notionnelles introduisent l'insécurité en droit. On ajoutera que la généralisation du « *cloud computing* » abolit définitivement les frontières et met à mal, du moins dans leur effectivité, les règles nationales. Au final, ne pourrions-nous pas nous demander si la **réglementation technologiquement neutre** d'Internet et de ses services, réglementation aux concepts souples et plus ou moins malléables, ne suscite pas des difficultés tout aussi grandes d'application, et on dénonce en ce sens les conséquences s'ensuivant sur le plan de la sécurité juridique, qu'une réglementation qui serait plus spécifique aux

réseaux sociaux ? La première laisse en tous cas au juge plus de matière pour combler un « vide » juridique dont on tenterait de lui démontrer l'existence. « Plus de matière » car nous le savons, il n'existe pas de vide juridique, ne fût-ce qu'en raison de la prohibition du déni de justice. Il n'empêche, dans tous les cas, du point de vue des acteurs d'Internet, de l'insécurité juridique subsiste – est-elle évitable[161] ?

40. Au-delà, nos réflexions laissent entrevoir que la question essentielle que le droit aura à résoudre est celle des libertés. Le réseau social est le lieu idéal de promotion des libertés : liberté de communiquer, liberté de s'informer et de connaître, liberté de se mouvoir, liberté de communiquer, liberté d'entreprendre, liberté d'association. Ces libertés sont fragilisées par le contrôle et par la multiplication des traces que nous laissons de l'exercice de ces libertés. Ce contrôle permet de mieux nous cerner, nous « profiler », nous tracer dans nos déplacements tant virtuels que physiques. Le danger vient non seulement de ces opérateurs privés surpuissants qui mettent en place des technologies dont la face cachée nous échappe que de la volonté des Etats qui trouvent dans ce réservoir sans précédents d'informations, les preuves de nos infractions. Les tentations sont grandes tant pour les uns que pour les autres d'exploiter ces gisements de données à caractère personnel. Vis-à-vis des entreprises, le consentement apparaît comme une protection bien fragile et même si l'espoir de voir un règlement européen mieux encadrer certaines dérives liées à ces modes d'exploitation nouveaux de données à caractère personnel (ainsi, la réglementation du profilage, la consécration du droit à l'oubli et de la portabilité des données), il est permis de s'interroger sur la façon dont ces règles pourront être effectives. Le principe de la légalité des preuves, principe jusqu'il y a peu sacro-saint en matière de procédure pénale, s'effrite chaque jour au nom de la sécurité dite « publique ». L'inquiétude face à ces contrôles croissants de nos activités sur les réseaux sociaux explique à la fois ce mouvement croissant de méfiance par rapport à leur utilisation, la normalisation des messages et,

(161) Même la mise en place, en droit de l'Internet, d'une sorte de régime général et transitoire – en attente que l'on (le législateur ou le juge) tranche une coutroverse légitime – du doute raisonnable (ou substantiel voire manifeste) : si vous avez des motifs raisonnables de croire de bonne foi que la réglementation ne vous lie pas mais que toutefois une certaine interprétation, dont la validité peut raisonnablement être questionnée, pourrait vous y lier, alors parmi ses dispositions seules celles pointées par la loi comme étant les plus essentielles devront être appliquées. Il s'agirait là d'une sorte d'application « allégée » d'un certain principe de précaution qui toutefois porterait également une certaine insécurité juridique – comment évaluer ce doute sans qu'il ne conduise toujours ou jamais à l'application de la loi en cause ?

chez certains, l'abandon de l'outil. Que conclure sinon que la protection effective et renforcée de notre vie privée conçue comme autodétermination informationnelle est sans doute la meilleure garantie de l'ensemble de nos libertés que nos réseaux sociaux entendent promouvoir ?